

DOCKET NO.: 260977US6PCT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Sung Yoon KIM, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/08178

INTERNATIONAL FILING DATE: June 4, 2004

FOR: INFORMATION DEVICE, INFORMATION SERVER, INFORMATION PROCESSING
SYSTEM, INFORMATION PROCESSING METHOD AND INFORMATION PROCESSING
PROGRAM

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that
the applicant claims as priority:

<u>COUNTRY</u>	<u>APPLICATION NO</u>	<u>DAY/MONTH/YEAR</u>
Japan	2003-163968	09 June 2003

Certified copies of the corresponding Convention application(s) were submitted to the
International Bureau in PCT Application No. PCT/JP04/08178.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)

04. 6. 2004

日本国特許庁
JAPAN PATENT OFFICE

REC'D PCT/PTO

13 JAN 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 6月 9日
Date of Application:

出願番号 特願2003-163968
Application Number:
[ST. 10/C]: [JP2003-163968]

出願人 ソニー株式会社
Applicant(s):

REC'D 24 JUN 2004

WIPO

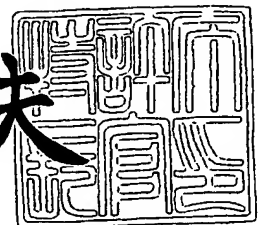
PCT

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 3月 3日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



BEST AVAILABLE COPY

出証番号 出証特2004-3016338

【書類名】 特許願

【整理番号】 0390168806

【提出日】 平成15年 6月 9日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 07/00
G09C 01/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 金 成潤

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 土屋 健一

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100098785

【弁理士】

【氏名又は名称】 藤島 洋一郎

【手数料の表示】

【予納台帳番号】 019482

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708092

【プルーフの要否】

要

【書類名】 明細書

【発明の名称】 情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラム

【特許請求の範囲】

【請求項 1】 暗号化されて配布され、ライセンスの保持を条件として利用可能になるコンテンツを記憶する第 1 の記憶手段と、

ライセンスを記憶する第 2 の記憶手段と、

コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶する第 3 の記憶手段と、

前記第 2 および第 3 の記憶手段の記憶内容に基づいて、前記第 1 の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段と

を備えたことを特徴とする情報機器。

【請求項 2】 前記第 1 の記憶手段は、前記コンテンツの利用を可能にするライセンスを識別するためのライセンス識別情報を、このコンテンツに対応付けて記憶しており、

前記第 2 の記憶手段に記憶されたライセンスは、前記ライセンス識別情報と前記グループ化機器識別情報とを含んでいる

ことを特徴とする請求項 1 に記載の情報機器。

【請求項 3】 前記再生処理手段は、

再生要求がなされたコンテンツに対応するライセンス識別情報を前記第 1 の記憶手段から読み出し、

読み出されたライセンス識別情報に対応するグループ化機器識別情報を前記第 2 の記憶手段から読み出し、

読み出されたグループ化機器識別情報に対応する鍵情報を前記第 3 の記憶手段から読み出し、

読み出された鍵情報を用いて、前記第 1 の記憶手段に記憶されたコンテンツを解読して出力する

ことを特徴とする請求項2に記載の情報機器。

【請求項4】 前記情報サーバに対し、自己の属する機器グループを情報サーバに登録することを要求するグループ登録要求を行うグループ登録要求手段とを備えたことを特徴とする請求項1に記載の情報機器。

【請求項5】 前記情報サーバに対して、その情報機器をサービス提供対象として登録し前記グループ化機器識別情報および前記鍵情報を送付することを要求するサービス登録要求を行うサービス登録要求手段を備えたことを特徴とする請求項4に記載の情報機器。

【請求項6】 自己を他から識別するための固有の機器識別情報を記憶する第4の記憶手段と、

前記情報サーバに対して、前記第4の記憶手段に記憶された機器識別情報を情報サーバに登録することを要求する機器登録要求を行う機器登録要求手段とを備えたことを特徴とする請求項4に記載の情報機器。

【請求項7】 前記第4の記憶手段に記憶されるべき前記機器識別情報を生成する機器識別情報生成手段を備えたことを特徴とする請求項6に記載の情報機器。

【請求項8】 前記情報サーバに対して、前記第4の記憶手段に記憶された機器識別情報を情報サーバの登録から削除することを要求する機器登録削除要求を行う機器登録削除要求手段を備えたことを特徴とする請求項6に記載の情報機器。

【請求項9】 1つの機器グループが、1のユーザの保有する複数の情報機器からなるグループとして規定されている

ことを特徴とする請求項1に記載の情報機器。

【請求項10】 前記鍵情報は、最上層から最下層に向かって枝分かれしていく階層ツリー構造における各ノードに対応して規定され暗号化されたノードキーのうち、最下層のデバイスノードとしての自機器グループに割り当てられたデバイスノードキーに該当するものであり、

前記コンテンツは、前記階層ツリー構造における前記デバイスノードキーから最上層のノードキーであるルートキーに至る経路上の各ノードキーを用いて多重

に暗号化されたものであり、

前記再生処理手段は、デバイスノードキーとしての前記鍵情報を用いて、前記階層ツリー構造における最下層から最上層に至る経路上のノードキーを順次解読し、得られた前記ルートキーを用いて前記コンテンツを解読する

ことを特徴とする請求項 1 に記載の情報機器。

【請求項 11】 前記コンテンツは、さらに、前記ルートキーによって暗号化されたコンテンツキーを用いて暗号化されており、

前記再生処理手段は、さらに、前記ルートキーによって前記コンテンツキーを解読し、得られたコンテンツキーを用いて前記コンテンツを解読する

ことを特徴とする請求項 10 に記載の情報機器。

【請求項 12】 前記コンテンツは、テキストデータ、静止画像データ、動画像データ、音声データ、またはそれらを組み合わせてなるデータであることを特徴とする請求項 1 に記載の情報機器。

【請求項 13】 暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバであって、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する機器グループ内の複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するサービス登録処理手段と

を備えたことを特徴とする情報サーバ。

【請求項 14】 前記情報機器からの機器登録要求に応じて、その機器登録要求から、個々の情報機器を識別するための機器識別情報を抽出し、この機器識別情報を前記グループ識別子に対応付けて登録する機器登録管理手段と

を備えたことを特徴とする請求項 13 に記載の情報サーバ。

【請求項 1 5】 前記機器登録管理手段は、一の機器グループについて登録された機器識別情報の数が一定数に達した以降は、その機器グループに属する新たな情報機器からの機器登録要求を拒否する

ことを特徴とする請求項 1 4 に記載の情報サーバ。

【請求項 1 6】 前記機器登録管理手段は、前記情報機器からの機器登録削除要求に応じて、この機器登録削除要求により指定された機器識別情報を登録から削除する

ことを特徴とする請求項 1 4 に記載の情報サーバ。

【請求項 1 7】 情報機器からのライセンス要求に応じて、このライセンス要求によって指定されたライセンスを、そのライセンス要求をしてきた情報機器に提供するライセンス提供手段と、

前記ライセンス要求からグループ化機器識別情報を抽出し、その抽出されたグループ化機器識別情報が前記サービス登録処理手段によって登録されたものであるか否かを調べ、その結果に応じて、前記ライセンス提供手段によるライセンス提供に伴う課金処理を行うか否かを判定する課金処理手段と

を備えたことを特徴とする請求項 1 3 に記載の情報サーバ。

【請求項 1 8】 1 つの機器グループが、1 のユーザの保有する複数の情報機器からなるグループとして規定されている

ことを特徴とする請求項 1 3 に記載の情報サーバ。

【請求項 1 9】 暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバと、この情報サーバから通信回線を通じてサービスを受けるクライアントとしての情報機器とを含んで構成される情報処理システムであって、

前記情報サーバは、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化

して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するサービス登録処理手段と

を備え、

前記情報機器は、

コンテンツを記憶する第1の記憶手段と、

ライセンスを記憶する第2の記憶手段と、

前記情報サーバから付与された前記グループ化機器識別情報と前記鍵情報とを、前記グループ識別子と共に記憶する第3の記憶手段と、

前記第2および第3の記憶手段の記憶内容に基づいて、前記第1の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段と

を備えたことを特徴とする情報処理システム。

【請求項20】 暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバと、前記情報サーバからサービスを受けるクライアントとしての情報機器とを含む情報処理システムに適用される情報処理方法であって、

前記情報サーバにおいて、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録し、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与し、

前記情報機器において、

コンテンツとライセンスとを記憶し、

前記情報サーバから付与された前記グループ化機器識別情報と前記鍵情報とを

、前記グループ識別子と共に記憶し、

記憶されている前記ライセンスの内容と前記グループ化機器識別情報と前記鍵情報とに基づいて、記憶されている前記コンテンツを解読して再生する処理を行う

ことを特徴とする情報処理方法。

【請求項 21】 コンテンツを利用する機能を備えた情報機器に適用されるプログラムであって、

暗号化されて配布されライセンスの保持を条件として利用可能になるコンテンツを記憶するステップと、

ライセンスを記憶するステップと、

コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶するステップと、

前記第 2 および第 3 の記憶手段の記憶内容に基づいて、前記第 1 の記憶手段に記憶されたコンテンツを解読して再生する処理を行うステップと

を前記情報機器に実行させることを特徴とする情報処理プログラム。

【請求項 22】 暗号化されて配布されたコンテンツを利用可能にする機能を備えた情報サーバに適用されるプログラムであって、

コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するステップと、

前記情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とを前記グループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、前記一のグループ化機器識別情報と前記一の鍵情報とを付与するステップと

を前記情報サーバに実行させることを特徴とする情報処理プログラム。

【発明の詳細な説明】**【0001】****【発明の属する技術分野】**

本発明は、コンテンツを利用する機能を備えた情報機器、コンテンツの利用を許可するライセンスを発行する情報サーバ、そのような情報機器および情報サーバを含む情報処理システム、そのような情報処理システムに適用される情報処理方法、ならびにそのような情報機器および情報サーバに適用されるプログラムに関する。

【0002】**【従来の技術】**

近年、ユーザが、P C (Personal Computer) を利用してインターネット経由で自分自身が保持している音楽データ等のコンテンツを他のユーザに提供する一方、自分自身が保持していないコンテンツを他のユーザから提供してもらうという、コンテンツ交換システムが出現している。

【0003】

この種のシステムでは、理論的には、1つのコンテンツが存在すれば、他のすべてのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなる。その結果、そのコンテンツの著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴って本来受け取ることが可能なロイヤリティを受け取る機会を失うことになる。そこで、コンテンツの流通を妨げることなく、著作権者からライセンスを受けていないコンテンツが不正にコピーされて利用されることを防止することが社会的に要請されている。

【0004】

そのような要請に応じて、例えば下記の特許文献1に記載されているように、コンテンツの配布を自由に行うことができると共に、許可されたユーザのみがコンテンツを利用できるようにした、いわゆるO p e n M G X (商標) と呼ばれる技術が提案されている。

【0005】

この技術は、次のようなものである。クライアントは、暗号化されたコンテン

ッをコンテンツサーバから受け取る。コンテンツのヘッダには、そのコンテンツを利用するとき必要とされるライセンスを特定するためのライセンス特定情報が記述されている。クライアントは、ライセンス特定情報に基づいて、ライセンスサーバにライセンスを要求する。ライセンスサーバは、ライセンス要求を受け取ると、課金処理を行った後、該当するライセンスをクライアントに送信する。クライアントはライセンスを保持していることを条件として、コンテンツを復号し再生することができる。この技術によれば、コンテンツの配布を自由に行うことができる一方、許可されたユーザのみがコンテンツを利用できることとなるため、コンテンツの不正利用を防止しつつコンテンツの流通を促進することが可能である。

【0 0 0 6】**【特許文献 1】**

特開 2 0 0 2 - 3 5 9 6 1 6 号公報

【0 0 0 7】**【発明が解決しようとする課題】**

近年のインターネットの爆発的な普及と急速なブロードバンド化とにより、P C だけではなく、いわゆる C E 機器 (Consumer Electronics) と呼ばれる家電向け電子機器もまた直接ネットワークに繋がることになることが予測される。また、1 人で複数の P C やネットアクセス可能な C E 機器を持つようになると考えられる。

【0 0 0 8】

しかしながら、このように、個人が持つ複数の機器がネットワークに接続されるようになった場合、従来のようにコンテンツやライセンスをダウンロードした 1 つの機器でのみ一元管理するモデルでは、ユーザの使い勝手が悪くなる。例えば、あるユーザがあるコンテンツを自宅の P C でネットワークを介して購入したとする。そのコンテンツを外出先でポータブル機器により利用したいと考えたとき、もう一度そのコンテンツを購入せざるを得ない。

【0 0 0 9】

本発明はかかる問題点に鑑みてなされたもので、その目的は、コンテンツを正

当な手段で入手したユーザのみが再生可能となるように保護されたコンテンツをユーザが自己の情報機器によって取得した場合に、そのコンテンツを、そのユーザが所有する他の情報機器でも利用することが可能となるような情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラムを提供することにある。

【0010】

【課題を解決するための手段】

本発明の情報機器は、暗号化されて配布され、ライセンスの保持を条件として利用可能になるコンテンツを記憶する第1の記憶手段と、ライセンスを記憶する第2の記憶手段と、コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶する第3の記憶手段と、第2および第3の記憶手段の記憶内容に基づいて、第1の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段とを備えている。

【0011】

本発明の情報サーバは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する機器グループ内の複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するサービス登録処理手段とを備えている。

【0012】

本発明の情報処理方法は、情報サーバの側において、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録し、情報機器からのサー

ビス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与し、情報機器の側において、コンテンツとライセンスとを記憶し、情報サーバから付与されたグループ化機器識別情報と鍵情報とを、グループ識別子と共に記憶し、記憶されているライセンスの内容とグループ化機器識別情報と鍵情報とに基づいて、記憶されているコンテンツを解読して再生する処理を行うようにしたものである。

【0013】

本発明の情報処理システムは、情報サーバと情報機器とを含んで構成される。情報サーバは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するグループ登録処理手段と、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するサービス登録処理手段とを備え、情報機器は、コンテンツを記憶する第1の記憶手段と、ライセンスを記憶する第2の記憶手段と、情報サーバから付与されたグループ化機器識別情報と鍵情報とを、グループ識別子と共に記憶する第3の記憶手段と、第2および第3の記憶手段の記憶内容に基づいて、第1の記憶手段に記憶されたコンテンツを解読して再生する処理を行う再生処理手段とを備えている。

【0014】

本発明の第1の情報処理プログラムは、暗号化されて配布されライセンスの保持を条件として利用可能になるコンテンツを記憶するステップと、ライセンスを記憶するステップと、コンテンツを利用しようとする複数の情報機器をグループ化して識別するためのグループ化機器識別情報と、機器グループごとに共通に付

与されたコンテンツ解読用の鍵情報とを、機器グループごとに付与されたグループ識別子と共に記憶するステップと、第2および第3の記憶手段の記憶内容に基づいて、第1の記憶手段に記憶されたコンテンツを解読して再生する処理を行うステップとを情報機器に実行させるものである。

【0015】

本発明の第2の情報処理プログラムは、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報をグループ識別子に対応付けて登録するステップと、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、その情報機器が属する複数の情報機器をグループ化して識別するための一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するステップとを情報サーバに実行させるものである。

【0016】

本発明の情報機器または第1の情報処理プログラムでは、コンテンツとライセンスとが記憶されると共に、グループ化機器識別情報とコンテンツ解読用の鍵情報とがグループ識別子と共に記憶される。ライセンスに含まれる情報と、グループ化機器識別情報と、コンテンツ解読用の鍵情報と、グループ識別子とに基づいて、コンテンツが解読されて再生され、利用可能になる。

【0017】

本発明の情報サーバまたは第2の情報処理プログラムでは、情報機器からのグループ登録要求に応じてグループ登録処理が行われ、情報機器からのサービス登録要求に応じてサービス登録処理が行われる。グループ登録処理においては、登録対象の機器グループに関する情報がグループ識別子に対応付けられて登録される。サービス登録処理においては、登録を要求してきた情報機器が、サービス提供対象として登録される。また、サービス登録処理においては、一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とが、上記のグループ識別子に対応付けられて登録される。さらに、サービス登録処理においては、登録を要求し

てきた情報機器が属する機器グループ内のすべての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とが付与される。この結果、その機器グループ内のすべての情報機器が、同じグループ化機器識別情報および鍵情報をもつことになる。

【0 0 1 8】

本発明の情報処理システムまたは情報処理方法では、上記の情報機器または第1の情報処理プログラムの作用と、上記の情報サーバまたは第2の情報処理プログラムの作用の双方が具現化される。すなわち、1つの機器グループ内のすべての情報機器が同じグループ化機器識別情報および鍵情報をもつことになると共に、各情報機器においては、コンテンツが解読されて再生され、利用可能になる。

【0 0 1 9】

なお、本明細書において用いる用語の基本的意義は、以下の通りである。

【0 0 2 0】

「コンテンツ」とは、デジタル化され暗号化されて配布されたコンテンツ本体部分をいい、テキスト情報、静止画や動画等の画像情報、音声情報、およびそれらの組み合わせ等をいう。例えば、電子書籍や電子新聞等のようなテキスト情報と画像情報とを組み合わせたものや、ゲームプログラムのようなアプリケーションソフトウェア等も含む。配布の形態は問わず、インターネット等の通信回線を介してにより配信されたものでも、CD-ROM等の記録媒体によって配布されたものでも構わない。「コンテンツの利用」とは、凡そコンテンツが有する情報を役立つ（意味のある）形で用いることをいい、コンテンツを再生し、閲覧し、または実行する行為等を含む。

【0 0 2 1】

「情報機器」とは、専用のコンテンツ利用機器のほか、パーソナルコンピュータ（PC）等のような汎用のコンピュータも含む。以下の説明では、単に「機器」または「デバイス」ともいう。「情報サーバ」とは、ライセンスを提供するための装置をいい、広くワークステーションやPC等の情報処理装置を含む。

【0 0 2 2】

「ライセンス」とは、コンテンツの利用を可能ならしめるための利用権情報で

あり、利用条件を含むほか、それ自体を識別するためのライセンス識別情報等も含む。「機器グループ」とは、一群の情報機器をいう。一般的には、1ユーザが保有する複数の情報機器群に該当するが、必ずしもこれに限定されない。

【0023】

「グループ化機器識別情報」とは、グループ分けされた個々の情報機器がどの機器グループに属するかを示す、いわばグローバルな次元での（機器グループ間での）機器識別情報である。言い換えると、ある機器グループに属することを表示するために各情報機器に付与される情報である。したがって、ある1つの機器グループ内においては、すべての情報機器が同じグループ化機器識別情報をもつ。この情報は、ユーザからは認識できないセキュアな情報として取り扱われるので、通常のユーザにとっては、機器グループの内外を問わず情報機器間で移動やコピーをしたり、情報自体の改変を行うことはできない。以下の実施の形態では、リーフIDがその一具体例に対応する。

【0024】

「グループ識別子」とは、機器グループを形成するときに、便宜的に機器グループごとに付与される一種のラベル情報であり、ユーザから認識できる。既存の機器グループに情報機器を追加登録する際に利用される。ユーザ＝機器グループと考えたときには、一種のユーザ識別情報に相当する。以下の実施の形態では、グループIDがその一具体例に対応する。

【0025】

「機器識別情報」とは、1つの機器グループ内において個々の情報機器を識別するために用いられる、いわばローカルな次元での（機器グループ内での）機器識別情報である。製造や販売の段階で情報機器自体に最初から設定される場合のほか、乱数等を用いたソフトウェアによってあとから生成される場合もある。以下の実施の形態では、機器IDがその一具体例に対応する。

【0026】

「鍵情報」とは、暗号化されたコンテンツを解読した利用可能な状態にするための解読（復号）用のキーである。本発明では、機器グループごとに共通のキーが付与される。したがって、1つの機器グループ内においては、すべての情報機

器が同じキーをもつ。このキーは、ユーザからは認識できないセキュアな情報として取り扱われるので、通常のユーザにとっては、機器グループの内外を問わず情報機器間で移動やコピーをしたり、情報自体の改変を行うことはできない。以下の実施の形態では、デバイスノードキーDNKがその一具体例に対応する。

【0027】

「課金処理」とは、ライセンスの販売に対する対価を徴収するために必要な手続き（例えば、銀行決済のための手続き）をいう。

【0028】

「1のユーザ」…一般的には一個人としてのユーザを指すが、必ずしもこれに限定されない。ライセンサーが許容するのであれば、例えば、生計を共にする1つの家族全体や、1つの社会的組織を指すこともある。

【0029】

「ノード」は、枝分かれする地点（分岐点）のことであり、「ノードキー」は各ノードごとに設定される暗号化キーであり、直下のノードキーによって暗号化されている。「デバイスノード」とは、最下層のデバイス（本発明では機器グループ）に対応するノードをいい、「デバイスノードキー」とは、最下層のデバイスに対応して規定される暗号化キーであり、上記の「鍵情報」と同義である。本発明では、1つの機器グループ内の情報機器には同じデバイスノードキーが付与される。「ルートキー」とは、階層ツリー構造の頂点に位置する暗号化キーである。

【0030】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照して詳細に説明する。

【0031】

図1は、本発明の一実施の形態に係る情報機器および情報サーバを含む情報処理システムの全体構成を表すものである。なお、本発明の実施の形態に係る情報処理方法およびプログラムは、本実施の形態の情報処理システムによって具現化されるので、以下、併せて説明する。

【0032】

この情報処理システムは、コンテンツを利用するクライアントとしての情報機器 1-1～1-4 と、情報サーバ 4 とを含んで構成されたコンテンツ配信利用システムである。これらの情報機器 1-1～1-4 および情報サーバ 4 は、いずれもインターネット 2 に接続されている。情報サーバ 4 は、暗号化されたコンテンツを情報機器 1-1～1-4 に提供するコンテンツ提供機能と、提供されたコンテンツを利用するのに必要なライセンスを情報機器 1 に付与するライセンス提供機能と、情報機器 1-1～1-4 がこのコンテンツ配信利用サービスを受ける際にまず必要となるサービス登録（ユーザ登録）を行うサービス登録機能と、情報機器がライセンスを受け取った場合に、その情報機器に対して課金処理を行う課金機能とを備えている。サービス登録機能およびライセンス提供機能は、例えば、「OpenMGX」と呼ばれる著作権管理技術を用いて実現することができる。

【0033】

情報機器 1-1～1-4 のうち、情報機器 1-1～1-3 は、あるユーザが所有する情報機器群であり、1つの機器グループ 1G を構成している。一方、情報機器 1-4 は他のユーザの所有するものである。情報機器 1-1～1-4 は、コンテンツ再生機能を有する専用の機器であってもよいし、あるいは汎用の PC であってもよい。なお、以下の説明では、1つの情報機器は1つの機器グループにのみ所属するものとし、1つの情報機器が複数の機器グループに跨がって所属することはしないものとする。

【0034】

情報機器 1-1～1-3 は、所定の事前手続き（後述）を行うことにより、同一の機器グループ 1G に属するようになり、コンテンツおよびライセンスを相互に移動させてコンテンツおよびライセンスを利用することが可能である。情報機器 1-4 は機器グループ 1G に属していないので、コンテンツおよびライセンスを情報機器 1-1～1-3 から入手しても利用可能とはならない。同様に、情報機器 1-4 のコンテンツおよびライセンスを情報機器 1-1～1-3 が入手したとしても、利用可能とはならない。

【0035】

なお、この図の例においては、情報機器が4台のみ示されているが、実際には、任意の台数の情報機器がインターネット2に接続される。また、機器グループ1Gは3台の情報機器を含んでいるが、実際には任意の台数を含んでよい。また、この図では、1つの機器グループのみを示しているが、実際には、複数の機器グループが存在し得る。

【0036】

機器グループ1Gに含まれる各情報機器1-1～1-3は、それらの物理的同一性を問題とする立場に立った場合の情報サーバ4からすると、互いに別々のハードウェアであると認識されるが、コンテンツ利用ライセンスの有効性を管理する立場に立った場合の情報サーバ4からすると、コンテンツの利用を許可された互いに区別されない(個性のない)情報機器であると認識されるようになっていく。上記の物理的同一性は、各情報機器1-1～1-3がそれぞれ有する固有の機器識別情報(機器ID)に基づいて判断される。

【0037】

一方、上記のライセンスの有効性は、予め情報情報サーバ4から情報機器1-1～1-3にそれぞれ付与されるグループ化機器識別情報(以下、リーフIDともいう。)および鍵情報DNK(デバイスノードキー; Device Node Key)に基づいて判断され、管理される。すなわち、1つの機器グループ内の情報機器は、それぞれ、互いに異なる(少なくともその機器グループ内で重複しない)機器IDを有する一方、同一の(共通の)リーフIDと同一の(共通の)鍵情報DNKとを有する。これらのリーフIDおよび鍵情報DNKは、ユーザからは不可視(認識不可能)であるようにセキュアな情報として取り扱われるので、機器グループの内外を問わず、情報機器間での移動やコピーはできない。また、ユーザ自身はリーフIDを認識できないので、ユーザがなすべき各種の登録手続き等を可能ならしめるために、機器グループごとに、ユーザIDでもあるグループ識別子(グループID)が付与されて、運用されるようになっていく。なお、機器ID、リーフID、鍵情報DNKおよびグループIDについての詳細は後述する(図5、図6)。

【0038】

図2は情報機器1-1の一構成例を表すものである。

【0039】

図2に示したように、情報機器1-1は、CPU (Central ProcessingUnit) 21と、ROM (Read Only Memory) 22と、RAM (Random Access Memory) 23と、暗号化復号部24と、コーデック部25と、入出力インタフェース32とを備えている。これらは、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32を介して、入力部26と、出力部27と、記憶部28と、通信部29と、ドライブ30とが接続されている。

【0040】

CPU 21は、ROM 22に記憶されているプログラム、または記憶部28からRAM 23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU 21に供給する。RAM 23には、CPU 21が各種の処理を実行する上において必要なデータ等も適宜記憶される。

【0041】

暗号化復号部24は、既に暗号化されているコンテンツを解読（復号）する処理を行うためのものである。但し、後述するように、図2の構成が情報サーバ4に適用される場合には、暗号化復号部24はコンテンツを暗号化する機能を有する。コーデック部25は、例えば、ATRAC (Adaptive Transform Acoustic Coding) 3方式などで音楽コンテンツを圧縮（エンコード）して入出力インタフェース32に出力したり、逆に、入出力インタフェース32から入力され暗号化復号部24で解読された圧縮コンテンツを、再生可能なデータへと伸長（デコード）するためのものである。

【0042】

入力部26は、キーボードやマウス等よりなり、出力部27は、CRT（陰極線管）、LCD（液晶表示装置）等のディスプレイや、スピーカ等よりなる。記憶部28は、ハードディスク等により構成され、コンテンツやライセンスのほか、各種の管理情報を記憶する。通信部29は、モデムやターミナルアダプタ等より構成され、インターネット2を介して通信処理を行う機能を有する。具体的に

は、通信部 29 は、情報サーバ 4 に接続して暗号化されたコンテンツをダウンロードしたり、情報サーバ 4 と接続してライセンスのダウンロードや各種の登録手続き（後述）のための通信処理を行う。

【0043】

ドライブ 30 には、例えば、リムーバブルな磁気ディスク 41、光ディスク 42、光磁気ディスク 43、あるいは半導体メモリ 44 等の記憶媒体が着脱可能に装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部 28 にインストールされるようになっている。ドライブ 30 はまた、これらの記憶媒体からコンテンツを読み取ったり、逆に、これらの記憶媒体にコンテンツを記録する処理を行う場合もある。なお、光ディスク 42 には、CD-ROM (CompactDisk-Read Only Memory)、CD-R (Recordable)、CD-RW (ReWritable)、DVD (DigitalVersatileDisk) -ROM、DVD-RW、DVD+RW 等が含まれ、半導体メモリ 44 は、例えば、メモリスティック（商標）等により構成される。

【0044】

なお、他の情報機器 1-2 ~ 1-4 についても、図 2 に示した情報機器 1-1 と同じハードウェア構成を有する。また、図示は省略するが、情報サーバ 4 もまた、図 2 に示した情報機器 1-1 と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、必要に応じて、図 2 の構成を、情報サーバ 4 の構成としても引用するものとする。

【0045】

図 3 は、情報機器 1-1 の機能構成を表すものであり、本実施の形態におけるクライアント用の情報処理プログラムの基本構成に相当する。情報機器 1-1 の機能は、制御機能ブロック 50 と、通信機能ブロック 70 と、記憶機能ブロック 80 とに大別される。制御機能ブロック 50 は、再生処理機能 51 と、グループ登録要求機能 52 と、機器登録要求機能 53 と、サービス登録要求機能 54 と、機器登録削除要求機能 55 と、機器 ID 生成機能 56 と、コンテンツ・ライセンス要求機能 57 とを含む。記憶機能ブロック 80 は、第 1 の記憶部 81 ~ 第 4 の記憶部 84 を含む。

【0046】

制御機能ブロック50の各機能は主として図2のCPU21や暗号化復号部24等が担当する。通信機能ブロック70は主として図2の通信部29が担当し、記憶機能ブロック80の各機能は主として図2の記憶部28やRAM23が担当する。

【0047】

制御機能ブロック50の各機能の具体的内容は次の通りである。

【0048】

再生処理機能51は、第2の記憶部82および第3の記憶部83の記憶内容に基づいて、第1の記憶部81に記憶されたコンテンツを解読して再生するものである。グループ登録要求機能52は、情報サーバ4に対し、自機器（情報機器1-1）が属する機器グループを情報サーバ4に登録することを要求するグループ登録要求を行う機能である。機器登録要求機能53は、情報サーバ4に対し、第4の記憶部84に記憶された機器IDを情報サーバ4に登録することを要求する機器登録要求を行う機能である。サービス登録要求機能54は、情報サーバ4に対し、自機器をサービス提供対象として登録しリーフIDおよび鍵情報DNKを送付することを要求する機能である。機器登録削除要求機能55は、情報サーバ4に対して、第4の記憶部84に記憶された機器IDを情報サーバ4の登録から削除することを要求する機器登録削除要求を行う機能である。機器ID生成機能56は、機器登録要求機能53が必要とする機器IDを生成して、第4の記憶部84に記憶させる機能である。コンテンツ・ライセンス要求機能57は、情報サーバ4に対して、コンテンツやライセンスのダウンロードを要求する機能である。

【0049】

記憶機能ブロック80の各機能の内容は次の通りである。

【0050】

第1の記憶部81は情報サーバ4等から提供されたコンテンツを記憶する機能を有し、第2の記憶部82は情報サーバから提供されたライセンスを記憶する機能を有する。第3の記憶部83は、複数の情報機器をグループ化して識別するた

めのリーフIDと機器グループごとに共通に付与されたコンテンツ解読用の鍵情報DNKとを、機器グループごとに付与されたグループIDと共に記憶する機能である。図1の例では、リーフIDおよび鍵情報DNKは、ひとつのグループIDをもつ機器グループ1Gに含まれる情報機器1-1～1-3について共通化されたものである。第4の記憶部84は、自機器（情報機器1-1）を機器グループ1G内の他の情報機器1-2, 1-3から識別するための固有の機器IDを記憶する機能を有する。

【0051】

図4は、情報サーバ4の機能構成を表すものであり、本実施の形態におけるサーバ用の情報処理プログラムの基本構成に相当する。情報サーバ4の機能は、制御機能ブロック90と、通信機能ブロック100と、記憶機能ブロック110とに大別される。制御機能ブロック90は、コンテンツ・ライセンス提供機能94と、グループ登録処理機能91と、機器登録管理機能92と、サービス登録処理機能93と、課金処理機能95とを含む。記憶機能ブロック110は、コンテンツ蓄積部111と、ライセンステーブル112と、グループ管理テーブル113とを含む。

【0052】

制御機能ブロック90の各機能は主としてCPU21や暗号化復号化部24等が担当し、通信機能ブロック100は主として通信部29が担当し、記憶機能ブロック110は主として記憶部28やRAM23が担当する。

【0053】

制御機能ブロック50の各機能の具体的内容は次の通りである。

【0054】

コンテンツ・ライセンス提供機能94は、リーフIDを含むコンテンツ要求やライセンス要求を情報機器1-1等から受け付け、その要求されたコンテンツやライセンスを、その要求をしてきた情報機器に提供する機能である。

【0055】

グループ登録処理機能91は、コンテンツを利用しようとする情報機器からのグループ登録要求に応じて、その情報機器が属する機器グループに関する情報

(グループ情報) をグループ識別子に対応付けて登録する機能である。

【0056】

機器登録管理機能92は、情報機器からの機器登録要求に応じて、その機器登録要求から、個々の情報機器を識別するための機器識別情報を抽出し、この機器識別情報をグループ識別子に対応付けて登録する処理を行うほか、情報機器からの機器登録削除要求に応じて、この機器登録削除要求により指定された機器識別情報を登録から削除する処理を行う機能である。機器登録管理機能92はまた、ある機器グループについて登録された機器IDの数が一定数に達した以降は、新たな情報機器からの機器登録要求を拒否する処理を行う機能も含む。

【0057】

サービス登録処理機能93は、情報機器からのサービス登録要求に応じて、その情報機器をサービス提供対象として登録すると共に、リーフIDおよび鍵情報DNKをグループIDに対応付けてグループ管理テーブル113に登録し、さらに、その情報機器が属する機器グループ内のすべての情報機器に対して、その登録されたリーフIDおよび鍵情報DNKを付与する機能である。このサービス登録機能93は、本実施の形態では、「OpenMGX」登録処理が相当する。

【0058】

課金処理機能95は、情報機器よりなされたライセンス要求からリーフIDを抽出し、その抽出されたリーフIDがグループ登録機能により登録されているか否かを調べ、その結果に応じて、コンテンツ・ライセンス提供機能94によるライセンス提供に伴う課金処理を行うか否かを判定する機能である。

【0059】

記憶機能ブロック110の各機能の具体的内容は次の通りである。

【0060】

コンテンツ蓄積部111は、情報機器からの要求に応じて提供する多種多様なコンテンツを予め作成して蓄積するものである。ライセンステーブル112は、例えば図5(B)に示したように、各コンテンツに対応して用意されたライセンスのリストテーブルである。グループ管理テーブル113は、図5(A)に示したように、リーフIDと鍵情報DNKとをグループIDに対応付けて登録すると

共に、機器IDをリーフIDに対応付けて登録するものである。ライセンステーブル112およびグループ管理テーブル113については以下に詳述する。

【0061】

図5(A)は、グループ管理テーブル113の一例を表すものである。このグループ管理テーブル113には、グループID121に対応して、パスワード122と、グループ情報123と、機器ID124と、サービスデータ125とが互いに対応付けられて登録されている。なお、この図では、後述するトランザクションID(TID)の図示を省略している。ここで、グループID:パスワード:機器ID:サービスデータの対応関係は、1:1:n:1である。但し、nは正の整数である。

【0062】

グループID121およびパスワード122はグループ登録時に割り当てられ、機器ID124は機器登録時に割り当てられ、サービスデータ125はサービス登録時に割り当てられるようになっている。

【0063】

ここで、グループ登録とは、ユーザが機器グループ1Gによってコンテンツ配信サービスを利用するに当たり、始めに一度だけ行われる登録である。グループ登録を行うことにより、ユーザは、グループIDとパスワードとを取得し、これらを用いることにより、コンテンツ配信サービスにおける機器登録やコンテンツの購入等を行うことができるようになる。

【0064】

また、機器登録とは、あるユーザが所有する1つ以上の機器を1つのグループとしてサーバが管理するための処理である。

【0065】

サービス登録とは、機器登録の済んだ情報機器を用いてコンテンツを利用するに際して必要となる手続きであり、本来は、個々の情報機器とコンテンツ解読キーとを関連付けることにより、情報機器間での不正コピーによる利用を防止することを目的として行われる処理である。但し、本実施の形態では、グループ登録の済んだ機器グループ内においては、情報機器間でコンテンツやライセンスを自

由にコピーすることが許容される。

【0066】

なお、グループ登録、機器登録およびサービス登録の詳細は後述する。

【0067】

グループID121は、その機器グループそのものを特定し、他の機器グループから識別するためのものであり、いずれかの情報機器からのグループ登録要求に応じて、その要求をした情報機器の属する機器グループに付与される。本実施の形態のように、1ユーザが1機器グループに対応するようになっている場合には、このグループID121はユーザIDに相当する。パスワード122は、グループ登録の際に、グループID121と共に付与される。これらのグループID121およびパスワード122は、機器グループを形成するときに、情報サーバ4から便宜的に機器グループごとに付与される情報であり、ユーザからも認識可能である。ユーザは、既登録の機器グループに情報機器を追加登録する場合や機器登録を削除する場合に、入力を求められるようになっている。

【0068】

グループ情報123は、機器グループに関する情報であり、グループ登録時にユーザから提供される。本実施の形態のように、1ユーザが1機器グループに対応する場合には、グループ情報123はユーザの個人情報（ユーザの氏名、住所、電話番号、メールアドレス、クレジットカード番号等）に相当する。

【0069】

機器ID124は、1つの機器グループ内において個々の情報機器を識別するために用いられる、いわばローカルな次元での（機器グループ内での）機器識別情報である。すなわち、機器ID125は、ある機器グループ内の情報機器間で互いに異なるものとなっており、この点で、機器グループ内の情報機器に共通に付与されるリーフIDとは異なる。この機器ID125によって、機器グループに何台の情報機器が登録されているかが把握される。この機器ID125は、情報機器1-1が専用のコンテンツ再生機器の場合には、製造や販売の段階でROM22に設定されるが、情報機器1-1がPC等の汎用機の場合には、乱数等を用いたソフトウェアによってあとから（例えば、後述する機器登録時に）生成さ

れる。このようなソフトウェアは、例えばグループ登録時や機器登録時に情報サーバ4からダウンロードされ、図3の機器ID生成機能56を実現する。

【0070】

サービスデータ125は、リーフIDと鍵情報DNKとを含む。リーフIDは、コンテンツを利用しようとする複数の情報機器をグループ化して識別するために各情報機器に付与される情報であり、上記のように「グループ化機器識別情報」の一具体例に対応する。言い換えると、リーフIDは、ある機器グループに属することを表示するために各情報機器に付与される情報である。鍵情報DNKは、コンテンツ解読用のキーであり、後述する階層ツリー構造(図7)のノードのうち最下層のノードに付与されるリーフキーを含んで構成されたデバイスノードキーである(図8(B)～(D)参照)。機器グループごとに共通の鍵情報DNKが付与される。したがって、1つの機器グループ内においては、すべての情報機器が同じリーフIDと鍵情報DNKとをもつ。これらのリーフIDおよび鍵情報DNKを利用して運用することにより、1つの機器グループ内のすべての情報機器において、(ライセンスされた)コンテンツを自由に利用することが可能になる。なお、リーフIDおよび鍵情報DNKの意義については、後にさらに詳述する。

【0071】

図5(A)に示した例では、情報機器1-1～1-3からなる機器グループ1G(図1)に、「G₀」というグループIDと「ABCD」というパスワードが付されると共に、「L₀」というリーフIDと「DNK₀」という鍵情報DNKとが付与されている。この例では、機器グループ1Gに属する情報機器1-1～1-3が、それぞれ、D₀，D₁，D₂という機器IDを有するものとして登録されている状態を示している。

【0072】

図5(B)は、ライセンステーブル112の一例を表すものである。このライセンステーブル112には、ライセンスID127と、ライセンスの内容128と、ライセンスを付与した機器グループのグループID129とが対応付けられて登録されている。図5(B)に示した例では、例えば、「a b c d e f」とい

うライセンスIDのライセンスに対して、3つのグループID（「G₀」, 「G₁」, 「G₂」）が対応付けられており、これにより、これらのグループIDをもつ3つの機器グループにそのライセンスがそれぞれ提供されていることがわかる。

【0073】

図6は、情報機器1-1の記憶機能ブロック80（図3）により記憶されている情報の内容を表すものである。具体的には、例えば記憶部28（図2）の記憶内容である。なお、この図において、下線を付したものはユーザが認識し得る（見える）情報である。また、リーフIDや鍵情報DNKのように下線を付していないものはユーザからは認識できないセキュアな情報であり、ユーザがコピーや移動等の操作をすることはできないようになっている。

【0074】

記憶機能ブロック80は、コンテンツファイル130と、ライセンス140と、ユーザデータ150とを記憶する。これらの情報の記憶は、それぞれ、第1の記憶部81～第3の記憶部83によって担保されている。

【0075】

まず、コンテンツファイル130について説明する。このコンテンツファイル130は、ヘッダ（Header）部分とデータ（Data）部分とにより構成される。ヘッダ部分は、コンテンツ識別情報（コンテンツID）131と、デジタル権利管理情報（DRM; Digital Right Management）132と、ライセンス識別情報（ライセンスID）133と、有効化キーブロックEKB（Enabling Key Block）134と、暗号化されたコンテンツキー（以下、被暗号化コンテンツキーともいう。）135とを含んで構成されている。データ部分は、暗号化されたコンテンツ（以下、被暗号化コンテンツともいう。）136によって構成される。なお、この被暗号化コンテンツ136は、複数のブロックに分けて暗号化されている。

【0076】

コンテンツID131は、コンテンツ自体を特定または識別するための情報である。なお、このコンテンツID131に付随させて、そのコンテンツのコード

ック方式等の付随情報を設けるようにしてもよい。

【0077】

デジタル権利管理情報132は、コンテンツを使用する規則および状態 (Usage rules/status) や、情報サーバ4のウェブページのURL (Uniform Resource Locator) 等を含んでいる。使用規則および状態としては、例えば、コンテンツの再生回数やコピー回数等が記述される。URLは、情報機器1-1が情報サーバ4に対して、ライセンスID133で特定されるライセンスを取得する場合のほか、グループ登録要求、機器登録要求、サービス登録要求機器および登録削除要求を行うときに用いられる情報サーバ4のアドレス情報である。

【0078】

ライセンスID133は、被暗号化コンテンツ136を利用するときに必要とされるライセンスを識別するもので、図5(B)で説明したものと同一のものである。このライセンスID133によって、コンテンツファイル130とライセンス140とが結びつけられている。

【0079】

有効化キープブロックEKB134は、後述する階層ツリー構造(図7)の最下層ノードキー(リーフキー)から最上層ノードキー(ルートキーKR)に至る経路のうちの、少なくともルートキーKRを含む部分を暗号化してなるものであり、例えば図8(A)に示したような構成を有する。この有効化キープブロックEKB134と、情報サーバ4から付与される鍵情報DNKとを用いることにより、被暗号化コンテンツ136を解読できるようになっている。これについては図7および図8を参照して後述する。

【0080】

被暗号化コンテンツキー135は、有効化キープブロックEKB134から生成されるルートキーKRを用いてコンテンツキーKCを暗号化したものである。被暗号化コンテンツ136は、被暗号化コンテンツキー135を解読して得られるコンテンツキーKCを用いて暗号化されたものである。

【0081】

次に、ライセンス140について説明する。このライセンス140は、ライセ

ンスID141と、作成日時142と、有効期限143と、使用条件144と、リーフID145と、電子署名146とを含んでいる。リーフID145を含むことにより、ライセンス140はユーザデータ150と結びつけられている。なお、ライセンスID141およびリーフID145は、既に説明したものと同義である（図5参照）。

【0082】

作成日時142は、このライセンス140を作成した日時である。有効期限143は、このライセンス140に基づいて、コンテンツを使用することが可能な使用期限である。使用条件144には、そのライセンスに基づいてコンテンツをダウンロードすることが可能なダウンロード期限、そのライセンスに基づいてコンテンツをコピーすることが可能な回数（許されるコピー回数）、チェックアウト回数、最大チェックアウト回数、そのライセンスに基づいてコンテンツをCD-RW等の記録媒体やPD（Portable Device）等の情報機器に記録することができる権利、ライセンスを所有権（買い取り状態）に移行できる権利、使用ログをとる義務等を示す情報等が含まれる。

【0083】

次に、ユーザデータ150について説明する。ユーザデータ150は、機器ID151と、グループID152と、パスワード153と、トランザクションID（TID）154と、リーフID155と、鍵情報DNK156とを含んでいる。リーフID155を含むことにより、ユーザデータ150はライセンス140に結びつけられている。鍵情報DNK156を含んでいることにより、これを用いてコンテンツファイル130の利用が可能になる。TID154は、後述する図9等の各種登録手続きにおいて、各手続き間を相互に結びつけるために用いられるものであり、これにより、ユーザの便宜が図られる。

【0084】

なお、機器ID151、グループID152、パスワード153、リーフID155および鍵情報DNK156は、図5で説明したものと同義のものである。

【0085】

図7は、ブロードキャストインクリプション（Broadcast Encryption）方式の

原理に基づいて情報機器（デバイス）およびライセンスキー（コンテンツ解読用の鍵）を管理するために構築される階層ツリー構造Hの一例を表すものである。

【0086】

この管理方式では、各キーは、ツリー構造における丸印で示したノードにそれぞれ対応して規定される。すなわち、キーは、最上層のルートキーKRから最下層のリーフキー（leaf key）まで階層的なツリー構造をなしている。具体的には、最上層のルートノードに対応してルートキーKRが規定され、2層目のノードに対応してキーK0、K1が規定され、3層目のノードに対応してキーK00～K11が規定され、最下層のノードに対応してキーK000～K111が規定されている。例えば、キーK000およびキーK001の上位のキーはK00であり、キーK00およびキーK01の上位のキーはK0であり、キーK0およびキーK1の上位のキーはルートキーKRである。他のキーについても同様であり、いずれのリーフキーからでも、上の階層を遡ればルートキーKRに辿り着く構造になっている。上位のキーはその直下のキーによって暗号化されている。

【0087】

最下層のノードは、ツリー構造における枝葉の位置に当たるのでリーフ（Leaf）と呼ばれ、これに付されるキーK000～K111は、上記したようにリーフキーと呼ばれる。ここに示した例では、各リーフは、番号0から番号7までの8個の機器グループのそれぞれに対応する。各リーフキーは、後述するように（図8参照）、対応するリーフに付与される鍵情報DNKの一部をなしている。番号0から番号7までの8個の機器グループのそれぞれに対応して、鍵情報DNK（ここでは、DNK0～DNK7）が設定され、さらに、各機器グループの特定識別のために、リーフID（ここでは、LF0～LF7）が付与されている。機器グループは、それぞれ、1または2以上のデバイス（情報機器）により構成される。図7に示した例では、機器グループ[0]は3つのデバイス[0]，[1]，[2]により構成され、機器グループ[1]は2つのデバイス[3]，[4]により構成され、機器グループ[2]は4つのデバイス[5]，[6]，[7]，[8]により構成されている。その他の機器グループ[3]～[7]についても同様である。

【0088】

情報サーバ4から提供されるコンテンツは、階層ツリー構造における最下層のリーフキーから最上層のルートキーKRに至る経路上の各ノードキーを用いて多重に暗号化されている。このように多重的に暗号化されたコンテンツを解読して利用可能にするために、例えば図8に示したような構造の有効化キープロックEKBおよび鍵情報DNKが用いられる。

【0089】

図8(A)は、有効化キープロックEKBの一例を表すものである。ここに示した例では、有効化キープロックEKBは、 $Enc(K0, KR)$ および $Enc(K1, KR)$ という2つのデータにより構成されている。ここで、 $Enc(K0, KR)$ は、ルートキーKRをその直下のノードキーK0によって暗号化したデータであり、 $Enc(K1, KR)$ は、ルートキーKRをその直下のノードキーK1によって暗号化したデータである。

【0090】

図8(B)～(D)は、鍵情報DNKの一例を表すものである。(B)に示したように、機器グループ[0]に付与される鍵情報DNK₀は、 $Enc(K00, K0)$ 、 $Enc(K000, K00)$ およびリーフキーK000という3つのデータにより構成されている。 $Enc(K00, K0)$ は、ノードキーK0をその直下のノードキーK00によって暗号化したデータであり、 $Enc(K000, K00)$ は、ノードキーK00をその直下のリーフキーK000によって暗号化したデータである。(C)に示したように、機器グループ[1]に付与される鍵情報DNK₁は、 $Enc(K00, K0)$ 、 $Enc(K001, K00)$ およびリーフキーK001という3つのデータにより構成されている。 $Enc(K00, K0)$ は、ノードキーK0をその直下のノードキーK00によって暗号化したデータであり、 $Enc(K001, K00)$ は、ノードキーK00をその直下のリーフキーK001によって暗号化したデータである。(D)に示したように、機器グループ[2]に付与される鍵情報DNK₂は、 $Enc(K01, K0)$ 、 $Enc(K010, K01)$ およびリーフキーK010という3つのデータにより構成されている。 $Enc(K01, K0)$ は、ノードキーK0をその直下の

ノードキーK01によって暗号化したデータであり、Enc(K010, K01)は、ノードキーK00をその直下のリーフキーK010によって暗号化したデータである。その他の機器グループ[3]～[7]に付与される鍵情報DNK3～DNK7についても同様である（図示せず）。

【0091】

図7において、例えば、機器グループ[2]に着目すると、この機器グループ[2]に対応するリーフキーK010からルートキーKRに至る経路は、Enc(K010, K01), Enc(K01, K0), Enc(K0, KR)という3つのデータによって規定される。したがって、図8(A)に示した有効化キーブロックEKBと、図8(C)に示した鍵情報DNK2とを組み合わせることにより、階層ツリー構造における最下層から最上層に至る経路上のノードキーを順次解読してルートキーKRを取得し、得られたルートキーKRを用いてコンテンツを解読することができる。但し、図6に示したように、コンテンツは、ルートキーKRによって直接暗号化されているのではなく、ルートキーKRによって暗号化された被暗号化コンテンツキーEnc(KR, KC)を用いて暗号化されているので、実際には、ルートキーKRによってまず被暗号化コンテンツキーEnc(KR, KC)を解読し、得られたコンテンツキーKCを用いて被暗号化コンテンツEnc(KC, CONTENTS)を解読することにより、最終的なコンテンツCONTENTSを得ることになる。その他の機器グループについても同様である。

【0092】

結局、鍵情報DNK_i [i = 0～8] が付与されている機器グループに属する情報機器のみが、暗号を解読してコンテンツを利用できることになる。

【0093】

このように、本実施の形態では、ユーザが所有する1または2以上のデバイス（情報機器）をまとめて1つの機器グループとし、この機器グループを図7の階層ツリー構造における最下層のリーフノードに割り付けて、リーフIDと鍵情報DNKとを付与するようにしている。その結果、1つの機器グループ内のすべての情報機器に対して同じ（共通の）リーフIDおよび鍵情報DNKが付与される

ことになる。例えば、図 7 に示した例において、機器グループ [0] の 3 つのデバイス [0] ~ [2] には、同じリーフ ID (LF₀) および鍵情報 DNK₀ が付与され、機器グループ [1] の 2 つのデバイス [3], [4] には同じリーフ ID (LF₁) および鍵情報 DNK₁ が付与され、機器グループ [2] の 4 つのデバイス [5] ~ [8] には、同じリーフ ID (LF₂) および鍵情報 DNK₂ が付与される。その他の機器グループのデバイスについても同様である。

【0094】

次に、図 9 ~ 図 12 を参照して、以上のような構成の情報処理システムの動作を説明する。なお、図 9 ~ 図 12 は、情報機器 1-1, 1-2 と情報サーバ 4 との間で行われる一連のやりとりを表すものである。ここでは、情報機器 1-1 ~ 1-3 からなる機器グループ 1G を情報サーバ 4 に登録する場合を例に説明する。なお、以下の説明では、情報機器 1-1, 1-2 は、それぞれ、当初から機器 ID 1, ID 2 を有するものとして説明する。但し、既に述べたように、機器登録手続きの際に情報機器自身がソフトウェアによって機器 ID を生成して保持するようにしてもよい。

【0095】

まず、図 9 を参照して、情報機器 1-1 を用いて機器グループ 1G についてのグループ登録を行うと共に、情報機器 1-1 自身を、その登録した機器グループ 1G の一員として登録する場合の処理を説明する。

【0096】

情報機器 1-1 ではまず、グループ登録要求機能 52 (図 3) が、通信機能ブロック 70 を介して、情報サーバ 4 に対してグループ登録要求を行う (図 9: ステップ S201)。このグループ登録要求は、情報サーバ 4 のウェブページにアクセスすることにより行われる。このウェブページにおいて、ユーザが、登録しようとする機器グループに関するグループ情報 (ここでは、例えば、ユーザの住所、氏名、電話番号、メールアドレス等のユーザ情報) を入力部 26 (図 2) から入力し、送信ボタン (図示せず) をクリックすると、このグループ情報がグループ登録要求と共に通信機能ブロック 70 を介して情報サーバ 4 に送信される。

【0097】

情報サーバ4では、通信機能ブロック100を介して情報機器1-1からグループ登録要求を受け取ると、グループ登録処理機能91（図4）が起動して、グループ登録要求からグループ情報を抽出すると共に、グループIDおよびパスワードを発行し、これらをグループ情報と共にグループ管理テーブル（図5（A））に登録する。そして、グループ登録処理機能91は、発行したグループIDおよびパスワードをグループ登録完了通知と共に通信機能ブロック100を介して情報機器1-1に送信する（ステップS202）。

【0098】

情報機器1-1では、情報サーバ4から通信機能ブロック70を介してグループ登録完了通知を受け取ると、グループ登録要求機能52が、そのグループ登録完了通知からグループIDおよびパスワードを抽出し、これらを第3の記憶部83のユーザデータ150（図6）に格納する。

【0099】

次に、情報機器1-1では、機器登録要求機能53が、通信機能ブロック70を介して、情報サーバ4に対して機器登録要求を行う（ステップS203）。この機器登録要求は、ユーザが情報サーバ4のウェブページにアクセスして、グループIDおよびパスワードを入力部26（図2）から入力し、送信ボタンをクリックすることにより行われる。このとき、機器登録要求機能53は、ユーザデータ150（図6）から機器ID1を読み出し、この機器IDを、グループIDおよびパスワードと共に通信機能ブロック70を介して情報サーバ4に送信する。

【0100】

情報サーバ4では、通信機能ブロック100を介して情報機器1-1から機器登録要求を受け取ると、機器登録管理機能92（図4）が起動して、機器登録要求から機器ID1を抽出し、この機器ID1を、グループIDに対応付けてグループ管理テーブル113（図5（A））に登録する。このとき、機器登録管理機能92は、現在の処理（機器登録処理）と次の段階の処理（サーバ登録処理）とを関連付けるためのトランザクションID1（TID1）を発行し、機器ID1に対応付けてグループ管理テーブル113（図5（A））に登録する。そして、機器登録管理機能92は、通信機能ブロック100を介して情報機器1-1に対

し、発行したT I D 1と共に機器登録完了を送信する（ステップS 2 0 4）。なお、T I D 1は、後述するように、それ以降の手続きにおけるユーザの入力負担を軽減するために用いられるものである。なお、後述するように、機器登録可能な最大機器数を越えている場合、機器登録管理機能9 2は、その旨を情報機器1 - 1に送信する。

【0 1 0 1】

情報機器1 - 1では、情報サーバ4から通信機能ブロック7 0を介して機器登録完了通知を受け取ると、機器登録要求機能5 3が、その機器登録完了通知からT I D 1を抽出し、このT I D 1を、第3の記憶部8 3のユーザデータ1 5 0（図6）に格納する。

【0 1 0 2】

この段階で、情報サーバ4では、サービス登録処理機能9 3が起動し、通信機能ブロック1 0 0を介して、機器登録を完了した情報機器1 - 1に対してサービス登録（例えば、上記した「O p e n M G X」に基づく登録）を促す通知を行う（ステップS 2 0 5）。

【0 1 0 3】

サービス登録を促す通知を受けた情報機器1 - 1では、サービス登録要求機能5 4が起動し、情報サーバ4に対して通信機能ブロック7 0を介してサービス登録要求を行う（ステップS 2 0 6）。このサービス登録要求は、例えば、情報サーバ4から送られてきたサービス登録用のウェブページにおいて、ユーザが同意ボタン（図示せず）をクリックすることにより行われる。すなわち、ユーザのクリック操作に応じ、サービス登録要求機能5 4は、ユーザデータ1 5 0（図6）からT I D 1を読み出し、サービス登録要求と共に情報サーバ4に送信する。したがって、ユーザは、更めてグループIDおよびパスワードを入力する必要はない。

【0 1 0 4】

情報サーバ4では、通信機能ブロック1 0 0を介して情報機器1 - 1からサービス登録要求を受け取ると、サービス登録処理機能9 3（図4）が起動して、サービス登録要求からT I D 1を抽出し、抽出したT I D 1を基に、どの情報機器

からのサービス登録要求であるか、および、このサービス登録要求をしてきた情報機器を所有するユーザがサービス登録を済ましてあるか否かを判断する。ここでは、グループ登録の済んでいない機器グループに属する情報機器 1-1 からの要求であると判断し、リーフ ID と鍵情報 DNK とを発行すると共に、これらを、情報機器 1-1 のグループ ID に対応付けてグループ管理テーブル 113 (図 5 (A)) に登録する。そして、サービス登録処理機能 93 は、情報機器 1-1 に対して、リーフ ID と鍵情報 DNK とを含むサービスデータを、サービス登録完了通知と共に通信機能ブロック 100 を介して送信する (ステップ S207)。

【0105】

情報機器 1-1 では、通信機能ブロック 70 を介して情報サーバ 4 からサービス登録完了通知を受け取ると、サービス登録要求機能 54 が、そのサービス登録完了通知から、リーフ ID および鍵情報 DNK を含むサービスデータを抽出し、このサービスデータを、グループ ID と共に第 3 の記憶部 83 のユーザデータ 150 (図 6) にセキュアに (安全かつ秘密裏に) 保存する。この段階で、情報機器 1-1 にとってコンテンツの利用に必要なすべての事前登録が完了する。したがって、これ以降、ユーザは、情報機器 1-1 を介して情報サーバ 4 にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ 1G 内の他の情報機器 1-2 等によりダウンロードして取得したコンテンツおよびライセンスを情報機器 1-1 にコピーして利用することが可能となる。その詳細は後述する。

【0106】

次に、図 10 を参照して、情報機器 1-2 を機器グループ 1G の一員に加える場合の処理を説明する。この処理は、基本的に、情報機器 1-1 を機器グループ 1G の一員に加える場合の処理 (ステップ S203 ~ S207) とほぼ同様であるので、同様の記載は適宜省略する。

【0107】

まず、情報機器 1-2 では、機器登録要求機能 53 が、通信機能ブロック 70 を介して情報サーバ 4 に対して機器登録要求を行う (図 10 : ステップ S208

）。この機器登録要求は、ユーザが情報サーバ4のウェブページにアクセスして、情報機器1-1によって既に取得済のグループIDおよびパスワードを入力部26（図2）から入力し、送信ボタンをクリックすることにより行う。これにより、機器登録要求機能53は、ユーザデータ150（図6）から機器ID2を読み出し、この機器ID2を、ユーザが入力したグループIDおよびパスワードと共に情報サーバ4に送信する。このとき、機器登録要求機能53は、入力されたグループIDおよびパスワードを、機器ID2と共に第3の記憶部83（図3）のユーザデータ150（図6）に格納する。

【0108】

情報サーバ4では、通信機能ブロック100を介して情報機器1-2から機器登録要求を受け取ると、機器登録管理機能92が、機器登録要求から機器ID2を抽出し、この機器ID2を、グループIDに対応付けてグループ管理テーブル113（図5（A））に追加登録する。機器登録管理機能92はまた、トランザクションID2（TID2）を発行し、機器ID2に対応付けてグループ管理テーブル113に記憶する。そして、機器登録管理機能92は、情報機器1-2に対し、発行したTID2と共に通信機能ブロック100を介して機器登録完了を送信する（ステップS209）。なお、TID2は、上記のTID1と同様の目的で用いられるものである。

【0109】

情報機器1-2では、通信機能ブロック70を介して情報サーバ4から機器登録完了通知を受け取ると、機器登録要求機能53が、その機器登録完了通知からTID2を抽出し、このTID2を、第3の記憶部83のユーザデータ150（図6）に格納する。

【0110】

この段階で、情報サーバ4では、サービス登録処理機能93が起動し、通信機能ブロック100を介して、機器登録を完了した情報機器1-2に対して、サービス登録を促す通知を行う（ステップS210）。この通知は、例えばサービス登録用のウェブページを情報機器1-2に送信することで行う。

【0111】

サービス登録を促す通知を受けた情報機器 1-2 では、サービス登録要求機能 54 が起動して、通信機能ブロック 70 を介して、情報サーバ 4 に対するサービス登録要求を行う（ステップ S 2 1 1）。このサービス登録要求は、上記の情報機器 1-1 の場合と同様に、情報サーバ 4 から送られてきたサービス登録用のウェブページにおいて、ユーザが同意ボタン（図示せず）をクリックすることにより行われる。すなわち、ユーザのクリック操作に応じ、サービス登録要求機能 54 は、第 3 の記憶部 83 のユーザデータ 150（図 6）から T I D 2 を読み出し、これを、サービス登録要求と共に情報サーバ 4 に送信する。したがって、ユーザは、更めてグループ I D およびパスワードを入力する必要はない。

【0 1 1 2】

情報サーバ 4 では、通信機能ブロック 100 を介して情報機器 1-2 からサービス登録要求を受け取ると、サービス登録処理機能 93（図 4）が起動して、サービス登録要求から T I D 2 を抽出し、抽出した T I D 2 を基に、どの情報機器からのサービス登録要求であるか、および、グループ登録が済んでいるか否かを判断する。ここでは、グループ登録済の機器グループ 1 G に属する情報機器 1-2 からの要求であると判断し、グループ管理テーブル 113 から、情報機器 1-2 のグループ I D に対応して登録されているリーフ I D と鍵情報 D N K とを読み出し、これらを含むサービスデータを、サービス登録完了通知と共に通信機能ブロック 100 を介して送信する（ステップ S 2 1 2）。

【0 1 1 3】

情報機器 1-2 では、通信機能ブロック 70 を介して情報サーバ 4 からサービス登録完了通知を受け取ると、サービス登録要求機能 54 が、このサービス登録完了通知からリーフ I D および鍵情報 D N K を抽出し、これらの抽出情報を、第 3 の記憶部 83 のユーザデータ 150（図 6）に登録する。この段階で、情報機器 1-2 にとってコンテンツの利用に必要なすべての事前登録が完了する。したがって、これ以降、ユーザは、情報機器 1-2 を介して情報サーバ 4 にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ 1 G 内の他の情報機器 1-1 等によりダウンロードして取得したコンテンツおよびライセンスを情報機器 1-2 に

コピーして利用することが可能となる。その詳細は後述する。

【0114】

以下、同様にして、機器グループ1 G内の他の情報機器1-3についても、機器登録処理とサービス登録処理とを行うことにより、ユーザは、情報機器1-3を介して情報サーバ4にアクセスしてコンテンツおよびライセンスをダウンロードし、そのダウンロードしたコンテンツを利用したり、あるいは、機器グループ1 G内の他の情報機器1-1等によりダウンロードして取得したコンテンツおよびライセンスを情報機器1-3にコピーして利用することが可能となる。

【0115】

なお、本実施の形態では、トランザクションIDを利用して、機器登録手続きとさらに登録手続きとを関連付けるようにしたが、これは必ずしも必要ではなく、省略可能である。この場合には、サービス登録要求の際に（ステップS206）、ユーザに対してグループIDおよびパスワードの入力を求めるようにすればよい。

【0116】

このようにして、情報サーバ4は、ユーザが所有する複数の情報機器を束ねて1つの機器グループとして認識するようになるが、この機器登録を無制限に認めると、実質上、コンテンツの利用に制限がなくなり、ライセンサーの不利益が大きくなる。この弊害を回避するため、本実施の形態では、上記のように、1つの機器グループに含めることができる情報機器の数に制限を設けている。具体的には、情報サーバ4は、いずれかの情報機器から機器登録要求があった場合に、グループ管理テーブル113（図5（A））の1つの機器グループに登録されている機器IDの数をチェックし、この数が所定数nに達したときは、それ以降、機器登録要求を拒否し、その旨を情報機器に通知する。なお、通常、1人のユーザが登録できる情報機器の最大数は、配信サービスを行う事業者の運用ルールで決定される。

【0117】

また、例えば、ユーザが登録した情報機器の数が登録可能数の上限nまで達したのち、例えば、ユーザが所有する情報機器を買い換えた場合のように、他の新

たな情報機器を登録したい場合には、一旦、機器登録削除を行って登録機器の数を減らし、その後更めて、登録したい情報機器についての登録要求を行うようにすればよい。以下、この登録削除の手続きを図 1 1 を参照して説明する。ここでは、既に機器登録がなされている情報機器 1 - 2 についての登録削除を行う場合について説明する。

【0 1 1 8】

この場合、まず、情報機器 1 - 2 では、機器登録削除要求機能 5 5 が、情報サーバ 4 に対して機器登録削除要求を行う（図 1 1：ステップ S 2 1 3）。この機器登録削除要求は、ユーザが情報サーバ 4 のウェブページにアクセスして、既に取得済のグループ ID およびパスワードを入力し、送信ボタンをクリックすることにより行う。このとき、機器登録削除要求機能 5 5 は、ユーザデータ 1 5 0 から機器 ID 2 を読み出し、この機器 ID 2 を、ユーザが入力したグループ ID およびパスワードと共に情報サーバ 4 に送信する。

【0 1 1 9】

情報サーバ 4 では、情報機器 1 - 2 から機器登録削除要求を受け取ると、機器登録管理機能 9 2 が、機器登録要求から機器 ID 2 を抽出し、この機器 ID 2 を、グループ管理テーブル 1 1 3 から削除する。そして、機器登録管理機能 9 2 は、情報機器 1 - 2 に対し、機器登録削除完了通知を送信する（ステップ S 2 1 4）。

【0 1 2 0】

情報機器 1 - 2 では、情報サーバ 4 から機器登録削除完了通知を受け取ると、機器登録削除要求機能 5 5 が、第 3 の記憶部 8 3 のユーザデータ 1 5 0 から、リーフ ID および鍵情報 DNK を含むサービスデータを削除する。この結果、例えば図 1 1 の例では、グループ管理テーブル 1 1 3 に登録された機器 ID は、情報機器 1 - 1 についての機器 ID 1 のみとなり、情報機器 1 - 2 は機器グループ 1 G から外される。したがって、それ以降は、該当するコンテンツを情報機器 1 - 2 で利用することはできなくなる。

【0 1 2 1】

次に、図 1 2 を参照して、コンテンツおよびライセンスの提供・取得処理につ

いて説明する。なお、コンテンツは情報サーバ4の側に予め作り置きされており、グループ登録、機器登録およびサービス登録を済ましていない者やライセンスを取得していない者であっても、コンテンツ自体をダウンロードをすることはできるが、後述するように、それらの登録やライセンス取得をしていなければ、コンテンツの利用はできない。

【0122】

コンテンツのダウンロードを行う場合、情報機器1-1では、まず、ユーザの入力操作に応じて、コンテンツ・ライセンス要求機能57が起動し、通信機能ブロック70を介して、情報サーバ4に対して、コンテンツ要求を行う（図12：ステップS215）。具体的には、ユーザが入力部26を操作して、提供を受けようとするコンテンツを指定すると、コンテンツ・ライセンス要求機能57は、このコンテンツを指定する情報（コンテンツ指定情報）を取り込み、このコンテンツ指定情報を、コンテンツ要求と共に情報サーバ4に送信する。

【0123】

情報サーバ4では、情報機器1-1から通信機能ブロック100を介してコンテンツ要求を受け取ると、コンテンツ・ライセンス提供機能94が起動し、受け取ったコンテンツ要求からコンテンツ指定情報とを抽出する。コンテンツ・ライセンス提供機能94はさらに、コンテンツ蓄積部111から、その抽出したコンテンツ指定情報が指すコンテンツファイルを読み出し、その読み出したコンテンツファイルを、通信機能ブロック100を介して情報機器1-1に送信する（ステップS216）。

【0124】

情報機器1-1では、情報サーバ4から通信機能ブロック70を介してコンテンツファイルを受け取ると、コンテンツ・ライセンス要求機能57が、そのコンテンツファイルを第1の記憶部81に格納する。これにより、情報機器1-1は、図6に示したように、ライセンスIDによってライセンス140にリンクされたコンテンツファイル130を保有することとなる。

【0125】

次に、ライセンスの取得手順について説明する。ここではまず、情報機器1-

1を用いて情報サーバ4にアクセスしてライセンスを購入する場合について説明する。

【0126】

ライセンスを取得する場合、情報機器1-1では、まず、ユーザの入力操作に応じて、コンテンツ・ライセンス要求機能57が起動し、通信機能ブロック70を介して、情報サーバ4に対して、ライセンス要求を行う(図12:ステップS217)。具体的には、ユーザが入力部26を操作して、既に取得してあるグループIDとパスワードとを入力し、上記でダウンロードしたコンテンツを利用するのに必要なライセンスを指定すると、コンテンツ・ライセンス要求機能57は、そのライセンスを指定する情報(ライセンス指定情報)を取り込むと共に、ユーザデータ150(図6)からリーフIDを読み出し、このリーフIDおよびライセンス指定情報を、ライセンス要求と共に情報サーバ4に送信する。

【0127】

情報サーバ4では、情報機器1-1から通信機能ブロック100を介してライセンス要求を受け取ると、コンテンツ・ライセンス提供機能94が起動し、受け取ったライセンス要求からリーフIDとライセンス指定情報とを抽出する。コンテンツ・ライセンス提供機能94はさらに、ライセンステーブル112(図5(B))から、その抽出したライセンス指定情報に対応するライセンスIDおよびライセンスの内容を読み出し、これらに、ライセンス要求から抽出したリーフIDを付加する。ライセンスの内容には、バージョン、作成日時、有効期限および使用条件等の情報が含まれている。さらに、秘密鍵(図示せず)を用いて署名を付加することにより、図6に示したようなフォーマット形式のライセンス140を作成し、情報機器1-1に送信する(ステップS218)。このとき、コンテンツ・ライセンス提供機能94は、そのリーフIDに対応するグループID(この場合、情報機器1-1が属する機器グループ1GのグループID)を、グループ管理テーブル113(図5(A))から読み出し、このグループIDが、ライセンステーブル112中の該当する(提供しようとする)ライセンスIDに対応付けて登録されているか、否かを判断する。その結果、そのグループIDが登録されていない場合には、そのライセンスが未だ情報機器1-1によって購入され

ていないと判断し、そのグループIDを、ライセンステーブル112中の該当する（提供しようとする）ライセンスIDに対応付けて登録すると共に、課金処理機能95（図4）が課金処理を実行する。一方、そのグループIDが登録されている場合には、課金処理を行わない。ここで示した例では、対象としているライセンスの取得は、情報機器1-1が属する機器グループ1Gにおいて初めて行うものなので、ライセンスの購入と判断され、課金処理が行われる。

【0128】

情報機器1-1では、情報サーバ4から通信機能ブロック70を介してライセンスを受け取ると、コンテンツ・ライセンス要求機能57が、そのコンテンツファイルを第2の記憶部82に格納する。これにより、情報機器1-1は、図6に示したように、リーフIDによってユーザデータ150とリンクされたライセンス140を保有することとなる。したがって、これ以降、ユーザは、そのライセンスの示す条件の範囲内において、情報機器1-1を用いて、そのコンテンツを自由に利用することができる。

【0129】

なお、ライセンス取得処理は、コンテンツを取得する前に予め行っておくようにすることも可能である。

【0130】

次に、情報機器1-2から情報サーバ4にアクセスして、既に情報機器1-1が取得したものと同一ライセンスを取得する場合について説明する。

【0131】

この場合のライセンス取得処理は、基本的には、上記の情報機器1-1による処理と同様である。但し、この場合、機器グループ1G内でのライセンス取得は情報機器1-1に続いて2度目であるので、この点に関して、情報サーバ4は異なる処理を行う。すなわち、コンテンツ・ライセンス提供機能94は、情報機器1-2からのライセンス要求から抽出したリーフIDに対応するグループID（ここでは、情報機器1-2が属する機器グループ1GのグループID）を、グループ管理テーブル113（図5（A））から読み出し、このグループIDが、ライセンステーブル112中の該当する（提供しようとする）ライセンスIDに

対応付けて登録されているか、否かを判断する。ここでは、そのグループIDがライセンステーブル112に既に登録されているので、情報サーバ4の課金処理機能95（図4）は、課金処理を行わない。その他の処理は、情報機器1-1によるライセンス取得（購入）の場合と同様である。

【0132】

このように、ユーザは、情報機器1-1を用いて情報サーバ4から購入したライセンスと同一のライセンスを、機器グループ1G内の他の情報機器1-2を用いて、更めて料金を支払うことなく、情報サーバ4から再取得することが可能となる。このようなライセンスの再取得は、機器グループ1G内の別の情報機器1-3からも同様に行うことができ、料金はかからない。

【0133】

次に、図13を参照して、情報機器1-1を用いてコンテンツを再生する場合の処理について説明する。

【0134】

ユーザが入力部26を操作してコンテンツの再生を指示すると、再生処理機能51（図3）が起動し、その指定されたコンテンツに対応するライセンスID133を、第1の記憶部81に格納されているコンテンツファイル130（図6）から読み取る。再生処理機能51は、読み取ったライセンスID133に対応するライセンスが取得されているか否かを判定する。ライセンスが既に取得されていると判定された場合、再生処理機能51は、その取得されているライセンスが有効期限内のものであるか否かを判定する。なお、ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている有効期限143（図6）と、タイマ20により計時されている現在日時とを比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合には、ユーザにたいし、ライセンス更新処理の実行等を促す。

【0135】

次に、再生処理機能51は、読み取ったライセンスID133を基に、第2の記憶部82に格納されているライセンス140（図6）からリーフID145を読み取る。さらに、再生処理機能51は、読み取ったリーフIDを基に、第3の

記憶部 83 のユーザデータ 150 (図 6) から鍵情報 DNK 156 を読み取る。再生処理機能 51 は、この鍵情報 DNK 156 を用いて、コンテンツファイル 130 (図 6) の有効化キープブロック EKB 134 を解読して、ルートキー KR を得る。例えば、情報機器 1-1 が機器グループ [0] に属するものであるとすると、鍵情報 DNK₀ (図 8 (B) 参照) を用いて有効化キープブロック EKB (図 8 (A)) を解読する。具体的には、まず、鍵情報 DNK₀ の中のリーフキー K000 を用いて Enc (K000, K00) を解読してノードキー K00 を取得し、これにより得られたノードキー K00 を用いて Enc (K00, K0) を解読してノードキー K0 を取得し、これにより得られたノードキー K0 を用いて有効化キープブロック EKB の Enc (K0, KR) を解読してルートキー KR を取得する。再生処理機能 51 は、こうして得られたルートキー KR を用いて、被暗号化コンテンツキー 135 (= Enc (KR, KC)) を解読して、コンテンツキー KC を取得し、得られたコンテンツキー KC を用いて被暗号化コンテンツ 136 (= Enc (KC, CONTENTS)) を解読し、最終的に、利用可能な態様のコンテンツ CONTENTS を得る。再生処理機能 51 は、こうして解読したコンテンツを再生し、出力部 27 から出力する。

【0136】

情報機器 1-2, 1-3 を用いてコンテンツを再生する場合の処理も同様である。

【0137】

なお、情報機器 1-2, 1-3 に関しては、コンテンツおよびライセンスの取得方法が 2 通りある。第 1 の方法は、上記したように、情報サーバ 4 から直接ダウンロードする方法である。第 2 の方法は、情報機器 1-1 によって情報サーバ 4 からダウンロードしたコンテンツおよびライセンスを、そっくり情報機器 1-2 にコピーする方法である。これらのいずれの方法においても、情報機器 1-2, 1-3 は、取得したコンテンツを解読して再生することができる。なぜなら、これらの情報機器 1-2, 1-3 は、情報サーバ 4 に対する機器登録およびサービス登録をそれぞれ行ったことにより、コンテンツの再生に必要なサービスデータ (リーフ ID と鍵情報 DNK とを含む) を既に取り得し、保持しているからであ

る。

【0138】

以上のように、本実施の形態によれば、情報サーバにおいてユーザ（機器グループ）とその機器グループ内の各情報機器とを関連付けて管理し、同一ユーザの所有する情報機器には、同一のサービスデータ（リーフIDおよび鍵情報DNK）を書き込むことにより、ユーザの所有する複数の情報機器を1つのグループとして扱うようにしたので、同一グループ内の情報機器間では、同一のコンテンツおよびライセンスを利用することが可能となる。具体的には、例えば、ある情報機器のコンテンツおよびライセンスを、通常のファイルを操作する方法により、同一グループ内の別の情報機器にコピーすれば、その機器においてもコンテンツの再生が可能になる。すなわち、ユーザは、一旦、ある情報機器でコンテンツおよびライセンスをダウンロードしておけば、自己の所有する情報機器間に関する限り、通常のコピーを行うだけで、他の情報機器でコンテンツを利用することが可能になる。このため、それぞれの情報機器を何度もネットワークを介してサーバに接続してダウンロードする必要がなくなる。

【0139】

また、ある情報機器により情報サーバからコンテンツおよびライセンスを入手し、その後、同一グループ内の異なる情報機器によって、再び情報サーバから、その同じコンテンツおよびライセンスを入手することも可能である。その際には、課金処理は発生しない。これにより、例えばユーザが、利用したいコンテンツが保存されている自己の情報機器から遠く離れた場所にいる場合であっても、その時点で所有している他の情報機器によってコンテンツを利用することも可能となる。

【0140】

以上をまとめると、次のことが言える。

【0141】

(1) コンテンツを正当な方法で入手したユーザのみが再生可能となるように保護されたコンテンツを配信するシステムにおいて、ユーザがある情報機器で取得したコンテンツを、ユーザが所有する他の情報機器でも利用することが可能とな

る。

(2) ネットワークを介してサーバに接続するという方法ではなく、情報機器間で直接コンテンツやライセンスの移動が可能となる。

(3) コンテンツを入手した情報機器と同じグループに属する他の情報機器を用いて、ネットワークを経由して情報サーバから課金処理の発生なしにコンテンツおよびライセンスを入手することができる。

(4) ユーザが所有する情報機器を買い換えた場合においても、その新たな情報機器を用いて、入手済のコンテンツを利用することが可能となる。

【0142】

以上、実施の形態を挙げて本発明を説明したが、本発明はこの実施の形態に限定されず、種々の変形が可能である。例えば、上記実施の形態では、1つの情報サーバ4によって各種の登録処理等を行うようにしたが、コンテンツ提供処理、ライセンス提供処理、サービス登録処理および課金処理を互いに別の（物理機械的に独立した）サーバによって行うようにしてもよい。

【0143】

また、本実施の形態では、情報機器は情報サーバとの間でオンラインで各種の登録手続きやダウンロードを行うものとして説明したが、本発明はこれに限定されず、オフラインで登録手続き等を行うようにしてもよい。この場合には、例えば、コンテンツ、ライセンスおよび各種登録手続き用プログラムを、CD-R等のような可搬性の追記型記録媒体に収納して事業者がユーザに配布し、ユーザは、そのプログラムを自己の情報機器にインストールして実行させることにより、各種登録手続きと、コンテンツおよびライセンスの取得とを実現することができる。したがって、インターネット等の通信回線に接続し得る環境にない情報機器を有するユーザにも対応することができる。

【0144】

また、本実施の形態では、1のユーザは1の機器グループを登録できるものとして説明したが、1のユーザが複数の機器グループを登録できるようにしてもよい。なお、1のユーザは、一般的には一個人を指すが、必ずしもこれに限定されず、ライセンサーが許容するのであれば、例えば、生計を共にする1つの家族全

体や1つの社会的組織が1のユーザとなることができるようにしてもよい。さらには、1のユーザの内部を階層化して管理するようにしてもよい。例えば、1つの企業を1つのユーザとし、その企業内の複数の事業部をそれぞれサブユーザとする場合が該当する。この場合には、コンテンツやライセンスの種類や内容、性質、あるいは配布形態等に応じて、多様な管理態様や利用態様が想定され、実益があると考えられる。

【0145】

また、情報機器としては、様々な機器が想定される。例えば、電子書籍機器や電子辞書等の専用機器のほか、例えば、パーソナルコンピュータ等の汎用のコンピュータや、携帯電話等の汎用のPD機器にも適用可能である。専用機器としては、上記のほかに、例えば、CDやMD（商標）、あるいはICプレーヤ等のオーディオ再生機器、DVDに代表されるビデオ再生機器、さらには、HD内蔵のテレビジョン受像機やゲーム機等も含まれる。

【0146】

【発明の効果】

以上説明したように、本発明の情報機器または第1の情報処理プログラムによれば、コンテンツとライセンスとを記憶すると共に、グループ化機器識別情報とコンテンツ解読用の鍵情報とグループ識別子とを保有しておき、ライセンスに含まれる情報と、グループ化機器識別情報と、コンテンツ解読用の鍵情報と、グループ識別子とをリンクさせた処理を行うことによりコンテンツを解読するようにしたので、同じグループ化機器識別情報および鍵情報をもつ情報機器であれば、コンテンツを自由に利用可能になる。

【0147】

本発明の情報サーバまたは第2の情報処理プログラムによれば、情報機器からのグループ登録要求に応じて、登録対象の機器グループに関する情報をグループ識別子に対応付けて登録すると共に、情報機器からのサービス登録要求に応じて、登録を要求してきた情報機器をサービス提供対象として登録し、一のグループ化機器識別情報と一のコンテンツ解読用の鍵情報とをグループ識別子に対応付けて登録すると共に、登録を要求してきた情報機器が属する機器グループ内のすべ

ての情報機器に対して、一のグループ化機器識別情報と一の鍵情報とを付与するようにしたので、その機器グループ内のすべての情報機器が、同じグループ化機器識別情報および鍵情報をもつことになる。このため、機器グループ内のすべての情報機器においてコンテンツを自由に利用可能になる。すなわち、ユーザがある情報機器で取得したコンテンツを、ユーザが所有する他の情報機器でも利用することも可能となる。また、ネットワークを介してサーバに接続するという方法によるのではなく、情報機器間で直接コンテンツやライセンスを移動するという方法により、情報機器間でのコンテンツ利用が可能になる。

【0148】

特に、一旦登録された機器識別情報を情報サーバから削除することを情報機器が要求し、これに応じて、情報サーバがその登録削除を行うようにした場合には、ユーザが現に使用している情報機器を他の新たな情報機器に取り替えることも可能になる。

【0149】

また、情報機器が機器識別情報生成機能を備えるようにした場合には、機器識別情報が付与されていない既存の情報機器であっても、あとから機器識別情報を付与することができ、本発明が適用可能になる。

【0150】

また、一の機器グループについて登録された機器識別情報の数が一定数に達した以降は、情報サーバがその機器グループに属する新たな情報機器からの機器登録要求を拒否するようにした場合には、1つの機器グループに登録される情報機器の数が無制限に増えるのを防ぐことができる。

【0151】

また、ライセンス要求に応じてライセンスを情報機器に提供する際に、そのライセンス要求からグループ化機器識別情報を抽出すると共に、その抽出されたグループ化機器識別情報に基づいて、そのライセンスが、そのライセンス要求をしてきた情報機器の属する機器グループによって既に購入されたものであるか否かを調べ、その結果に応じて、ライセンス提供に伴う課金処理を行うか否かを判定するようにした場合には、機器グループ内の情報機器を用いてライセンスを一旦

購入しておけば、その機器グループ内の情報機器からライセンスを再取得する場合に、ライセンス料の再度の支払いを免れることができる。

【図面の簡単な説明】

【図 1】

本発明の一実施の形態に係る情報処理システムの全体構成を表すブロック図である。

【図 2】

情報機器および情報サーバの要部構成を表すブロック図である。

【図 3】

情報機器の機能構成の要部を表すブロック図である。

【図 4】

情報サーバの機能構成の要部を表すブロック図である。

【図 5】

情報サーバにおけるグループ管理テーブルおよびライセンステーブルの一例を表す図である。

【図 6】

情報機器におけるコンテンツファイル、ライセンスおよびユーザデータの内容の一例を表す図である。

【図 7】

情報サーバによって管理される暗号解読キーにおける階層ツリー構造の一例を表す図である。

【図 8】

図 8 の階層ツリー構造に適用される有効化キーブロックおよび鍵情報の内容の一例を表す図である。

【図 9】

情報機器と情報サーバとの間で行われるグループ登録処理、機器登録処理およびサービス登録処理を説明するための図である。

【図 1 0】

情報機器と情報サーバとの間で行われる機器登録処理およびサービス登録処理

を説明するための図である。

【図 1 1】

情報機器と情報サーバとの間で行われる機器登録削除処理を説明するための図である。

【図 1 2】

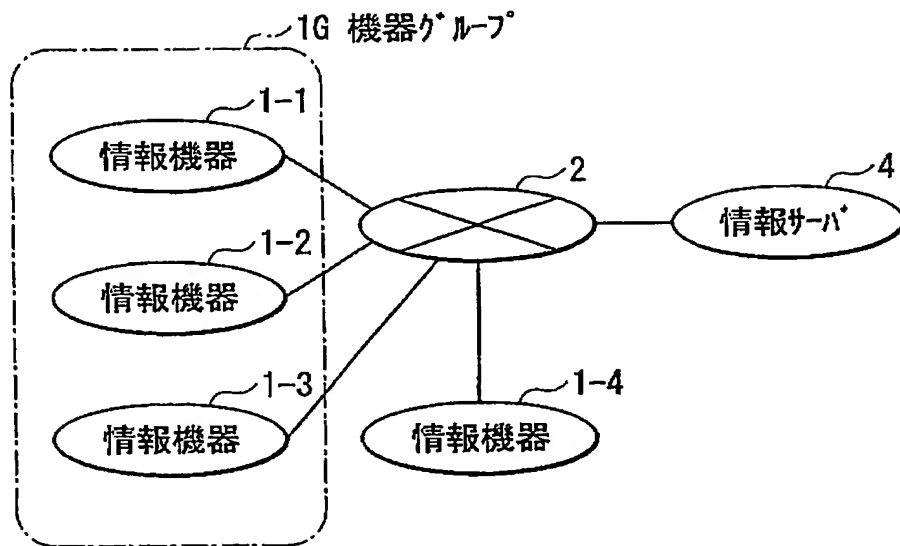
情報機器と情報サーバとの間で行われるコンテンツおよびライセンスのダウンロード処理を説明するための図である。

【符号の説明】

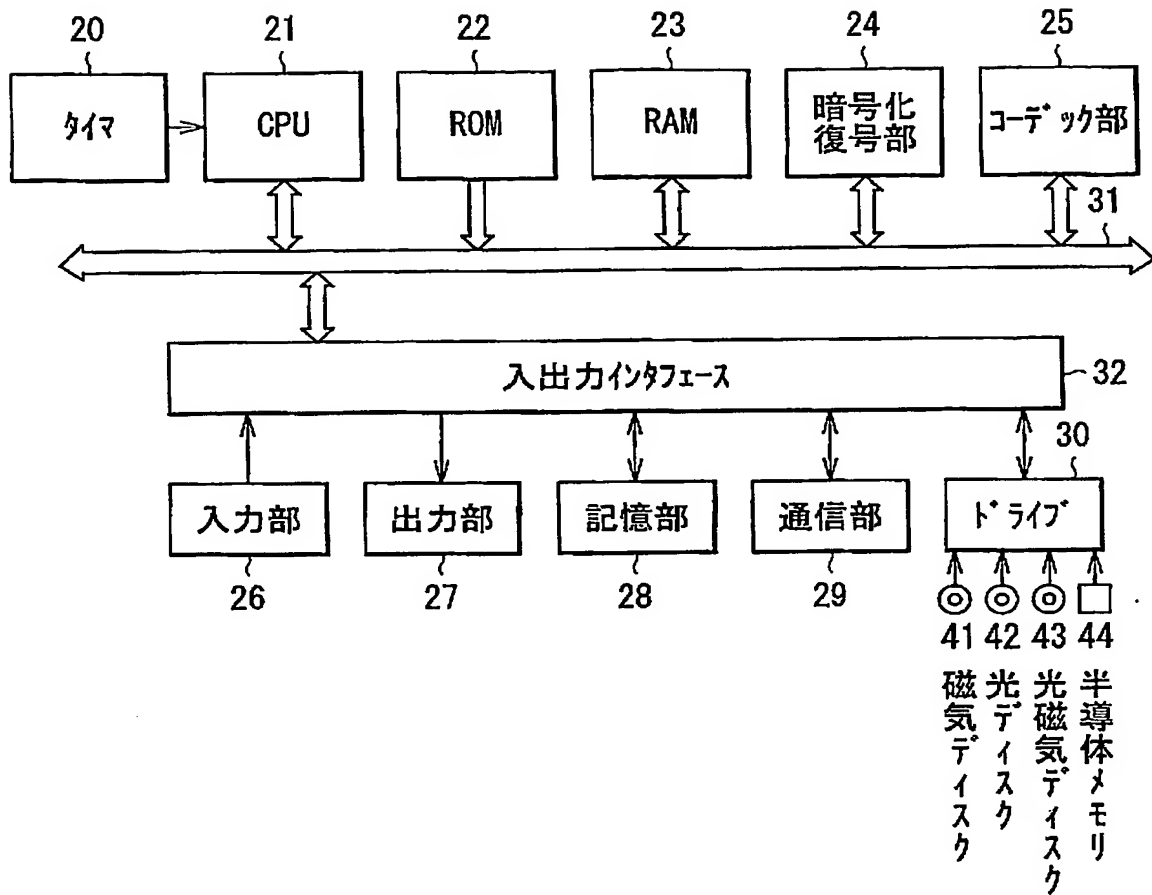
1-1~1-4…情報機器、1G…機器グループ、2…インターネット、4…情報サーバ、21…CPU、22…ROM、24…暗号化復号部、26…入力部、27…出力部、28…記憶部、29…通信部、50, 90…制御機能ブロック、51…再生処理機能、52…グループ登録要求機能、53…機器登録要求機能、54…サービス登録要求機能、55…コンテンツ・ライセンス提供機能、70, 100…通信機能ブロック、80, 110…記憶機能ブロック、81…第1の記憶部、82…第2の記憶部、83…第3の記憶部、84…第4の記憶部、91…グループ登録処理機能、92…機器登録管理機能、93…サービス登録処理機能、94…コンテンツ・ライセンス提供機能、95…課金処理機能、111…コンテンツ蓄積機能、112…ライセンステーブル、113…グループ管理テーブル、122…パスワード、123…グループ情報、124…機器ID、125…サービスデータ、127, 133, 141…ライセンスID、130…コンテンツファイル、131…コンテンツID、134…有効化キーブロックEKB、140…ライセンス、145, 155…リーフID、150…ユーザデータテーブル、152…グループID、156…鍵情報DNK。

【書類名】 図面

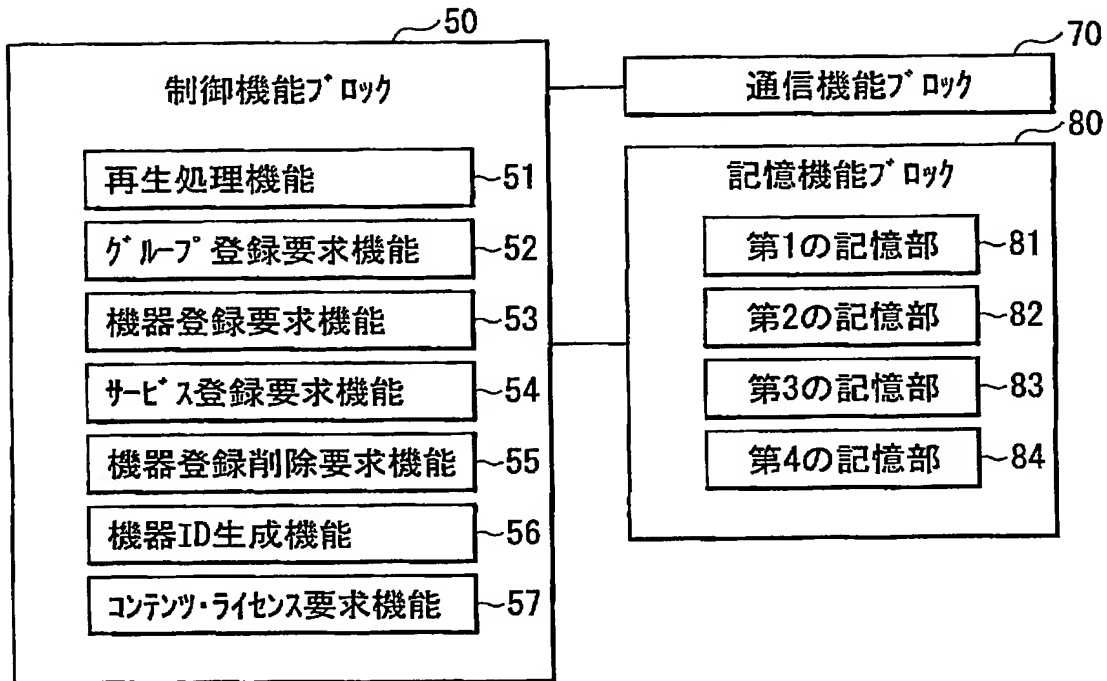
【図 1】



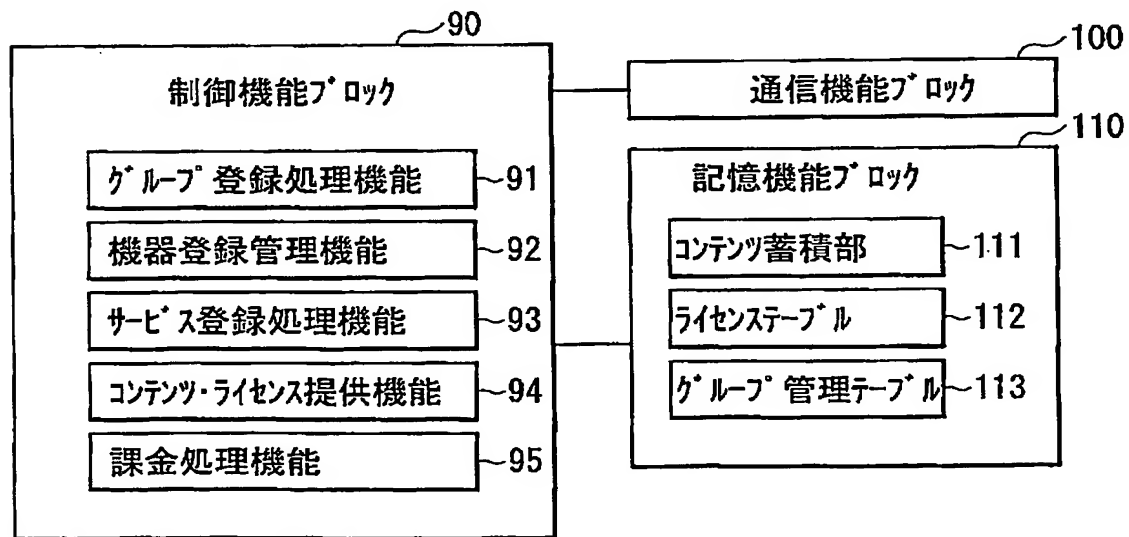
【図 2】



【図 3】



【図 4】



【図 5】

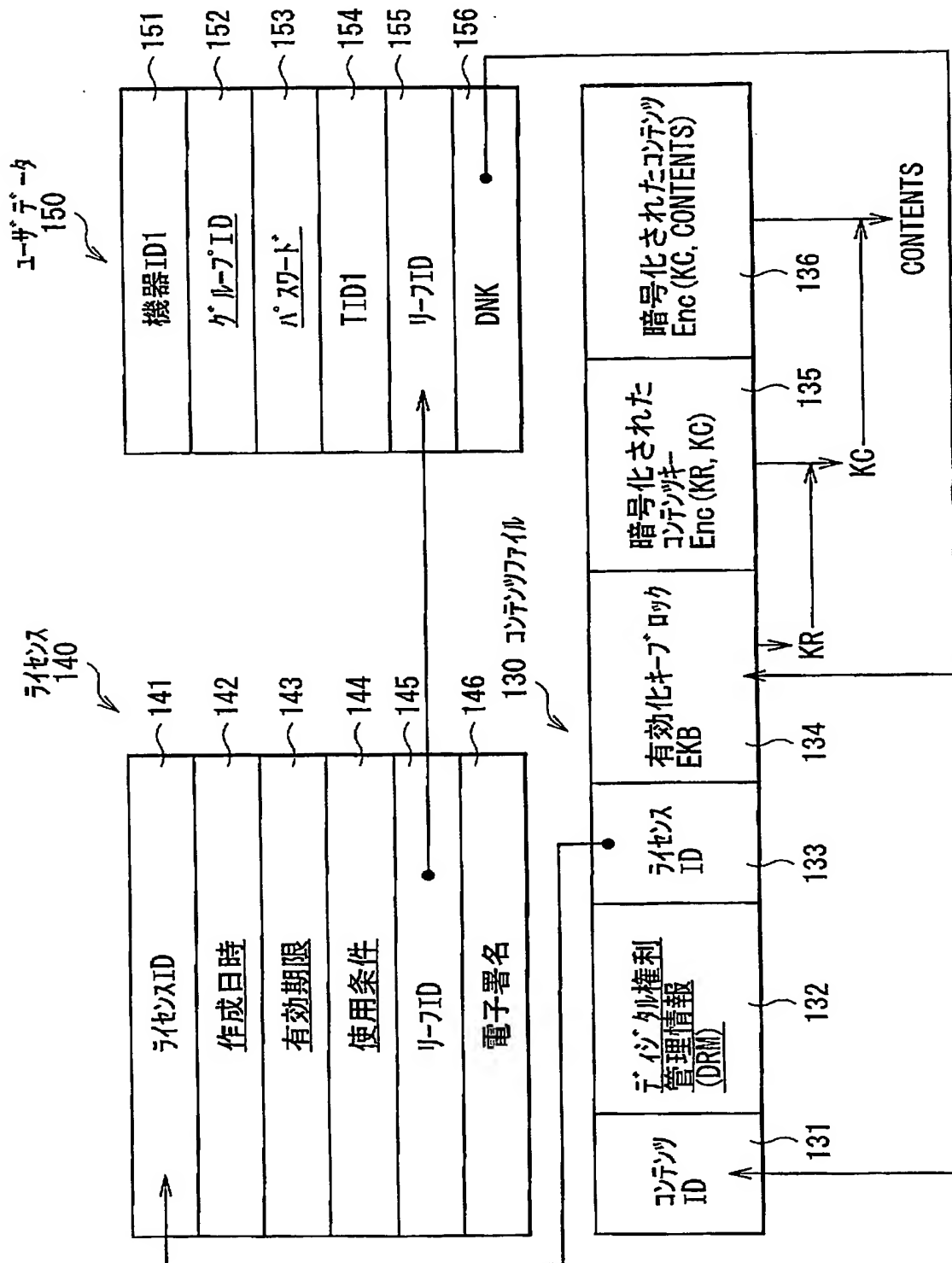
113 グループ管理テーブル

121 グループ ID	122 パスワード	123 グループ 情報	124 機器ID	125 サービスステータ	
				リーフID	DNK
G0	ABCD	○○○○	D0	LF0	DNK0
			D1		
			D2		
G1	EFGH	△△△△	D3	LF1	DNK1
			D4		
G2	IJKL	××××	D5	LF2	DNK2
			D6		
			D7		
			D8		
⋮	⋮	⋮	⋮	⋮	⋮

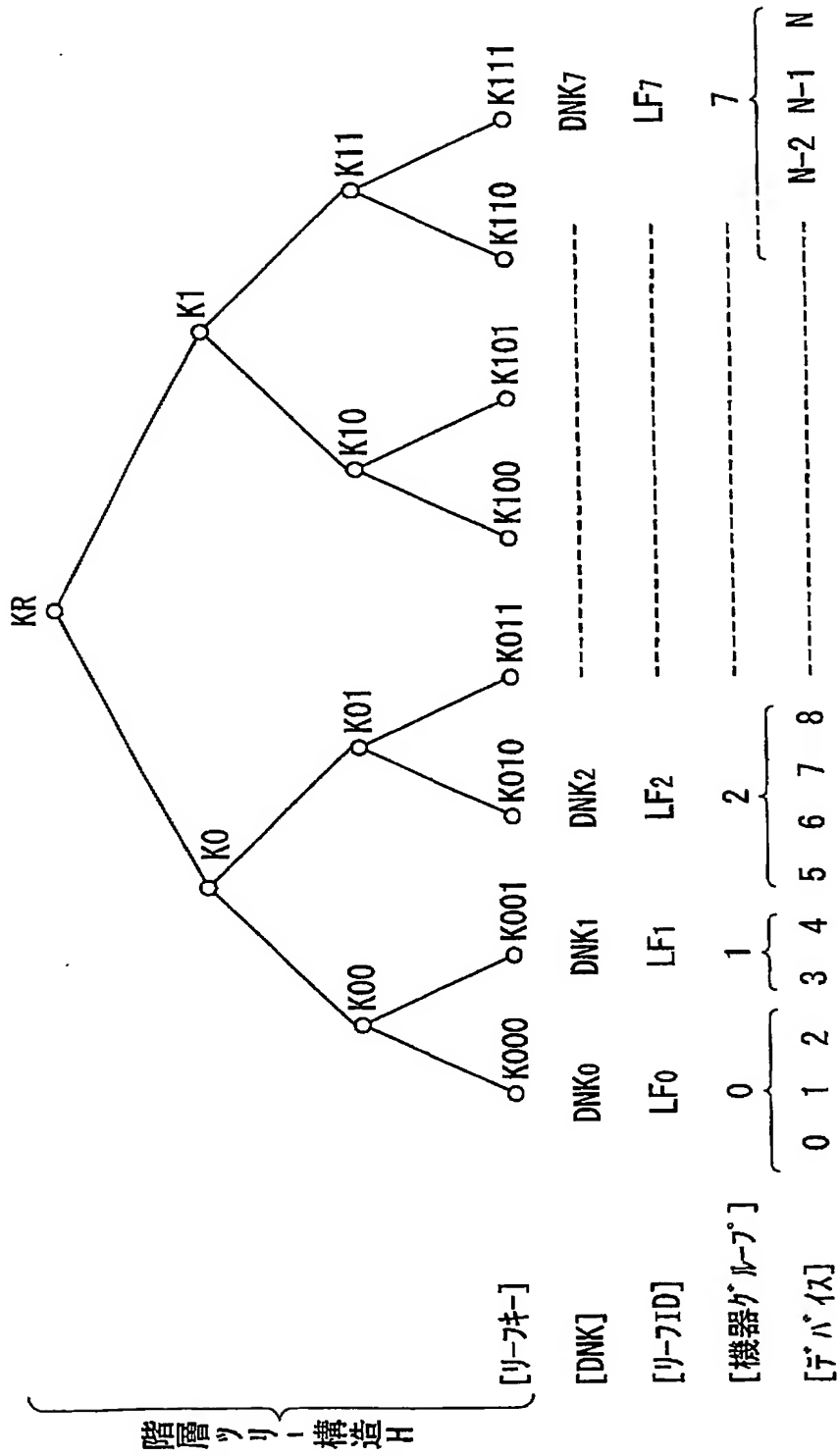
112 ライセンステーブル

127 ライセンスID	128 ライセンスの内容 (使用条件等)	129 ライセンスしたグループの グループ ID
abcdef	○○○○□□□□	G0, G1, G2
ghijkl	□□□○○○○	G0
mnopqr	△△○○△△○	G1
stuvws	△△△△○○○	G1
stuvws	××××△△△	G2
⋮	⋮	⋮

【図 6】



【図 7】



【図 8】

- (A) EKB=

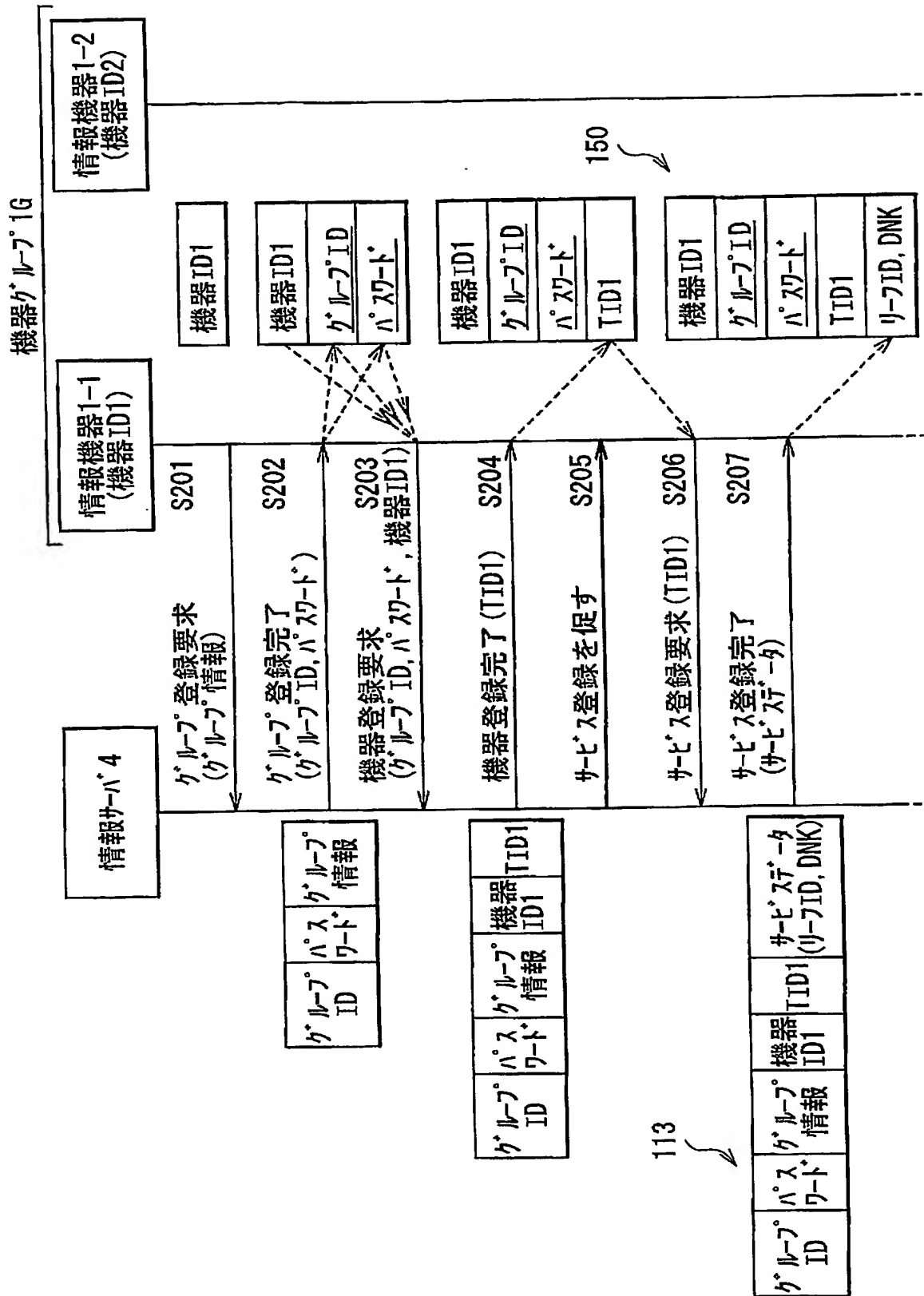
Enc (K0, KR)
Enc (K1, KR)
- (B) DNK0=

Enc (K00, K0)
Enc (K000, K00)
K000
- (C) DNK1=

Enc (K00, K0)
Enc (K001, K00)
K001
- (D) DNK2=

Enc (K01, K0)
Enc (K010, K01)
K010

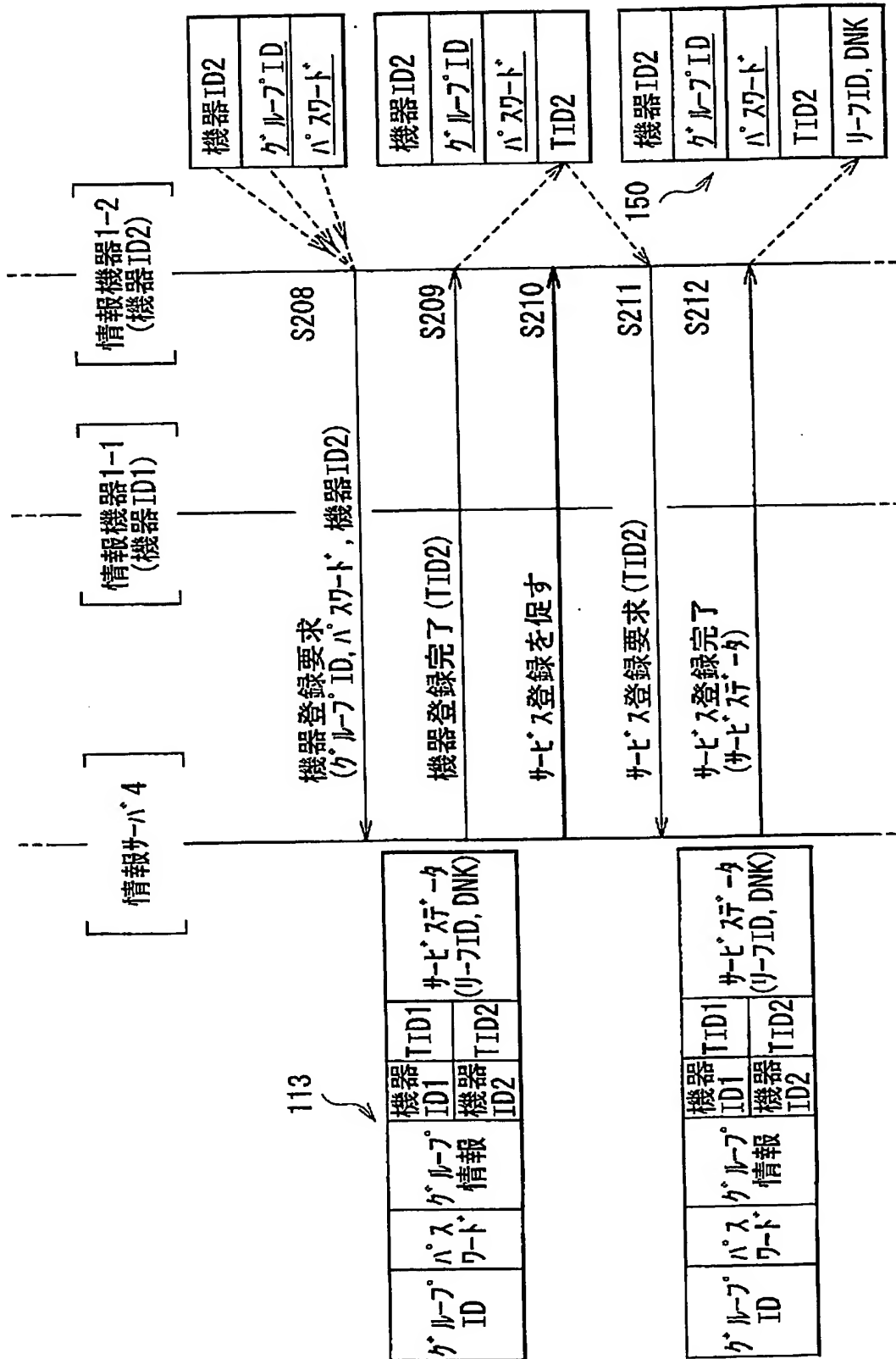
【図9】



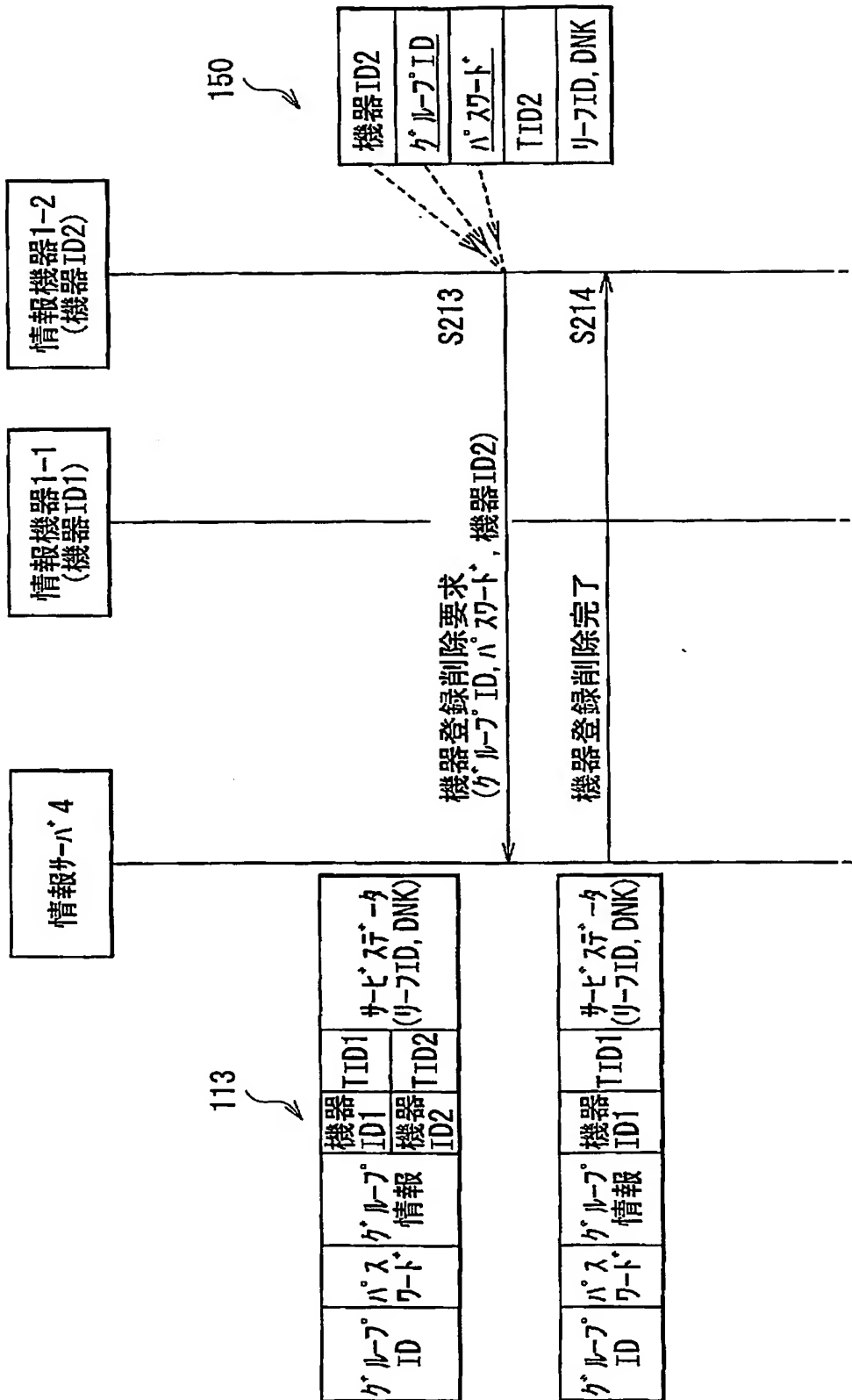
113

150

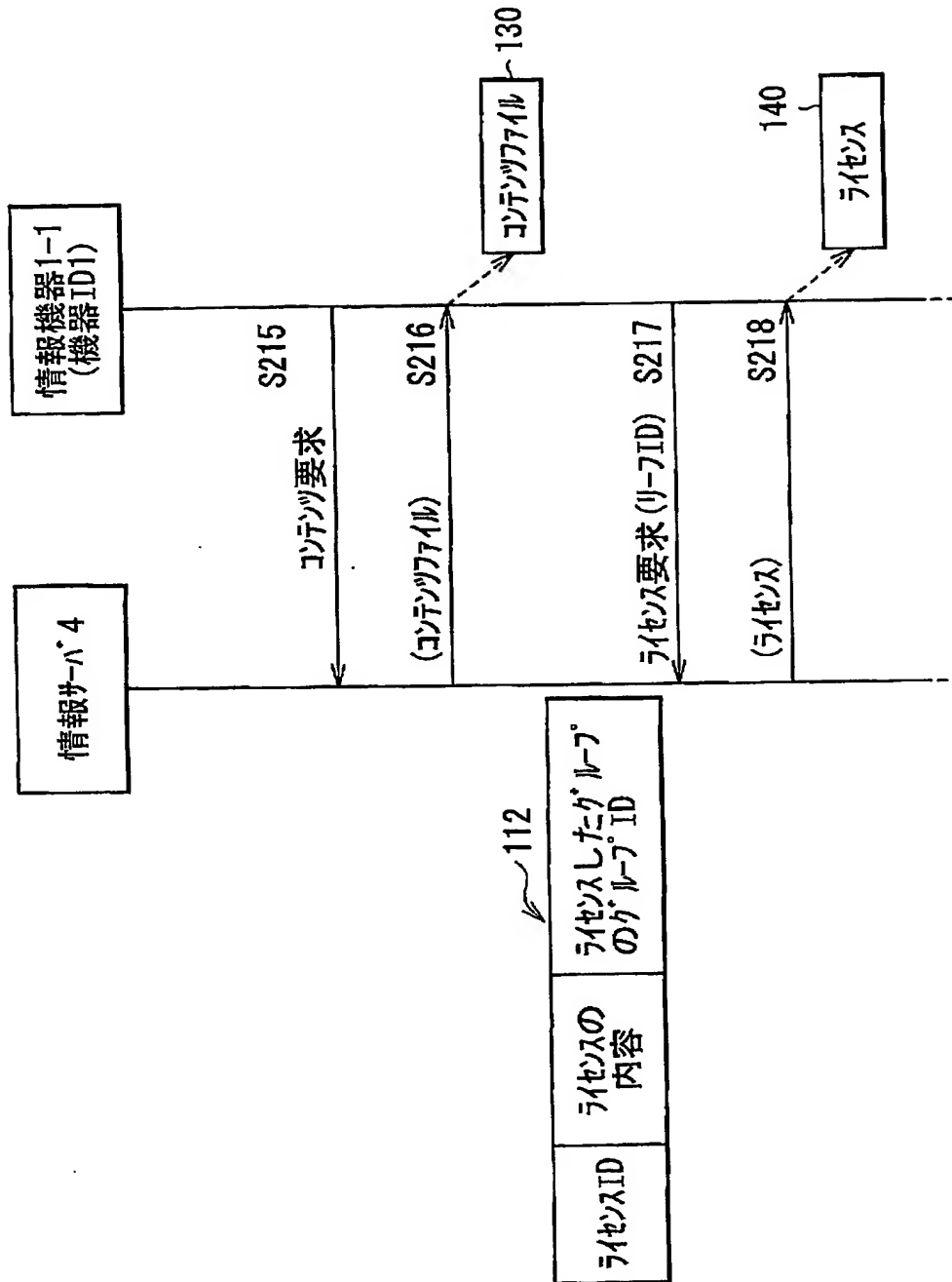
【図 10】



【図 11】



【図 12】



【書類名】 要約書

【要約】

【課題】 コンテンツを正当な手段で入手したユーザが、そのコンテンツを、そのユーザ所有の他の情報機器でも利用できるようにする情報機器、情報サーバ、情報処理システム、情報処理方法および情報処理プログラムを提供する。

【解決手段】 情報サーバ4は、ユーザと、そのユーザの所有する情報機器1-1～1-3のそれぞれとを関連付けて管理し、同一ユーザの所有する情報機器には、同一のサービスデータ（リーフIDおよび鍵情報DNK）を書き込むことにより、ユーザの所有する複数の情報機器を1つのグループとして扱う。この結果、ユーザ所有の情報機器1-1で取得したコンテンツを、ユーザ所有の他の情報機器1-2，1-3でも利用することも可能となる。また、情報機器1-1～1-3間で直接コンテンツやライセンスを移動するという方法により、それらの情報機器でのコンテンツ利用が可能になる。

【選択図】 図1

特願 2003-163968

出願人履歴情報

識別番号

[000002185]

1. 変更新月日
[変更理由]
住所
氏名

1990年 8月30日
新規登録
東京都品川区北品川6丁目7番35号
ソニー株式会社